(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 105224417 A
(43)申请公布日 2016.01.06

(21)申请号 201510519208.9

(22)申请日 2007.12.05

(30)优先权数据
60/873,153 2006.12.05 US

(62)分案原申请数据
200780050007.2 2007.12.05

(71)申请人 安全第一公司
地址 美国加利福尼亚

(72)发明人 D·马丁 里克·L·奥尔西尼
马克·S·奥黑尔

(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 杜文树

(51)Int.Cl.
*G06F 11/14*(2006.01)
*G06F 21/62*(2013.01)

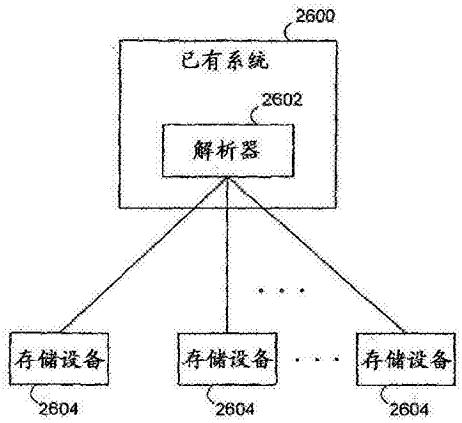
权利要求书2页 说明书63页 附图33页

(54)发明名称

改进的磁带备份方法

(57)摘要

本发明涉及一种改进的磁带备份方法。提供了一种可被集成到用于安全存储和传递数据的任意适合的系统中的安全数据解析器。安全数据解析器解析数据，然后将数据分割为被不同地存储或传递的多个部分。可以采用原始数据，所述数据部分或这两者的加密以提供附加的安全性。通过将原始数据分割为可被使用多个通信路径传递的数据部分，该安全数据解析器可用于保护运动中数据。




CN 105224417 A

1. 一种用于提供数据备份的方法，该方法包括：

在虚拟磁带备份系统处接收要被保持的磁带映象；

对磁带映象的内容执行加密操作并且基于密钥将磁带映象的内容分配到多个次级数据块，其中，所述多个次级数据块中的每个都包含磁带映象的各个子集的随机或伪随机分配，并且其中，所述密钥能够被用来确定将磁带映象的每个单位置于所述多个次级数据块中的哪个中；以及

通过访问指向虚拟磁带备份系统的多个物理存储设备的一个或多个逻辑安装点，将所述多个次级数据块存储在位于所述多个物理存储设备上的多个份中，

由此磁带映象能够被从小于全部的阈值数目的所述多个份恢复。

2. 根据权利要求 1 所述的方法，还包括在虚拟磁带备份系统处对磁带映象的内容编目录。

3. 根据权利要求 1 所述的方法，还包括将所述多个次级数据块发送到安全存储系统。

4. 根据权利要求 1 所述的方法，其中，所述物理存储设备包括磁带记录设备。

5. 根据权利要求 1 所述的方法，其中，所述物理存储设备包括硬盘驱动器。

6. 根据权利要求 1 所述的方法，其中，所述虚拟磁带备份系统包括在安全存储系统上执行的软件。

7. 根据权利要求 1 所述的方法，还包括虚拟磁带备份系统通过对由安全存储系统提供给虚拟磁带服务器的虚拟盘进行寻址，将磁带映象的内容发送到安全存储系统。

8. 根据权利要求 1 所述的方法，还包括从所述多个次级数据块之中至少阈值数目的次级数据块来重新构造磁带映象的内容。

9. 根据权利要求 1 所述的方法，其中，所述多个次级数据块对应于磁带映象的内容的一部分。

10. 根据权利要求 7 所述的方法，还包括将磁带映象的内容从虚拟磁带备份系统发送到客户机系统。

11. 一种磁带备份布置，包括：

虚拟磁带备份系统，其被配置为：

接收要被保持的磁带映象的内容；

对磁带映象的内容执行加密操作并且基于密钥将磁带映象的内容分配到多个次级数据块，其中，所述多个次级数据块中的每个都包含磁带映象的各个子集的随机或伪随机分配，并且其中，所述密钥能够被用来确定将磁带映象的每个单位置于所述多个次级数据块中的哪个中；以及

通过访问指向多个物理存储设备的一个或多个逻辑安装点，将所述多个次级数据块存储在位于所述多个物理存储设备上的多个份中，

由此磁带映象能够被从小于全部的阈值数目的所述多个份恢复。

12. 根据权利要求 11 所述的数据备份布置，其中，虚拟磁带备份系统被配置为从应用服务器接收磁带映象。

13. 根据权利要求 11 所述的数据备份布置，其中，所述物理存储设备包括磁带记录设备。

14. 根据权利要求 11 所述的数据备份布置，其中，所述物理存储设备包括硬盘驱动器。

15. 根据权利要求 11 所述的数据备份布置，其中，所述物理存储设备中的一个或多个位于远离虚拟磁带备份系统的位置。

16. 根据权利要求 11 所述的数据备份布置，其中，虚拟磁带备份系统还被配置为从所述多个次级数据块之中至少阈值数目的次级数据块来重新构造磁带映象的内容。

17. 根据权利要求 11 所述的数据备份布置，其中，所述多个次级数据块对应于磁带映象的内容的一部分。

18. 根据权利要求 16 所述的数据备份布置，其中，虚拟磁带备份系统还被配置为将磁带映象的内容从虚拟磁带备份系统发送到客户机系统。

19. 一种被配置为在数据备份布置内工作的安全存储系统，该安全存储系统包括被配置为执行程序指令的可编程电路，该程序指令在被执行时将安全存储系统配置为：

从虚拟磁带备份系统接收磁带映象的内容；

对磁带映象的内容执行加密操作并且基于密钥将磁带映象的内容分配到多个次级数据块，其中，所述多个次级数据块中的每个都包含磁带映象的各个子集的随机或伪随机分配，并且其中，所述密钥能够被用来确定将磁带映象的每个单位置于所述多个次级数据块中的哪个中；以及

通过访问指向虚拟磁带备份系统的多个物理存储设备的一个或多个逻辑安装点，将所述多个次级数据块存储在位于所述多个物理存储设备上的多个份中，

由此磁带映象能够被从小于全部的阈值数目的所述多个份恢复。

20. 根据权利要求 19 所述的安全存储系统，其中，所述物理存储设备包括磁带记录设备。

21. 根据权利要求 19 所述的安全存储系统，其中，所述物理存储设备包括硬盘驱动器。

# 改进的磁带备份方法

[0001] 本申请是本申请是中国专利申请号为200780050007.2、申请日为2007年12月05日的PCT申请PCT/US2007/025038的、名称为“改进的磁带备份方法”的发明专利申请的分案申请。

[0002] 与相关申请的交叉引用

[0003] 本申请要求提交于2006年12月5日的美国临时申请No.60/873,153的优先权，这里引用其完整内容作为参考。

## 技术领域

[0004] 本发明总体上涉及用于在备份磁带上备份数据的改进方法。

## 背景技术

[0005] 在当今社会中，个人和企业在计算机系统上和通过计算机系统进行活动的数目日益增多。这些计算机系统，包括专用和非专用计算机网络，通常存储，归档和传输各种类型的敏感信息。因此存在确保存储在这些系统上的以及在这些系统上传输的数据不能被读取或泄密的日益增加的需要。

[0006] 一种用于保护计算机系统安全的常见解决方案是提供登录和口令功能。然而，关于口令问题的大比例求助台呼叫已经证实口令管理是成本高昂的。另外，由于口令一般存储在例如通过暴力攻击易受不适当访问影响的文件内，口令提供很少的安全性。

[0007] 另一种保证计算机系统安全的解决方案是提供密码基础设施。密码术一般指通过将数据变换或加密为不可读格式保护数据。仅有拥有加密密钥（多个）的那些人可以将数据解密为可使用的格式。密码术用于识别用户，例如验证，以便允许访问特权例如授权，以便创建数字证书和签名等。一种流行的密码系统是公钥系统，公钥系统使用两个密钥，为公众所知的公钥和仅为个人或企业所有者所知的私钥。一般地，以一个密钥加密的数据被以另一个密钥解密，并且任意一个密钥都不可从另一个密钥重新创建。

[0008] 不幸的是，即使上面的典型公钥密码系统的安全性也高度依赖于用户。例如，密码系统例如通过用户浏览器将私钥发给用户。然后缺乏经验的用户一般将私钥存储在其他人通过开放计算机系统，诸如例如，Internet可访问的硬驱动器上。在另一方面，用户可能为包含其私钥的文件选择不好的名称，诸如例如“密钥”。上述和其他活动的结果是提供了密钥或多个密钥易于被危及的可能。

[0009] 除了上面的危险之外，用户可能将他或她的私钥存储在配置有归档或备份系统的计算机系统上，这潜在地导致私钥的拷贝经过多个计算机存储设备或其他系统。这种安全性缺口通常被称为“密钥迁移”。类似于密钥迁移，许多应用最多通过简单的登录和口令访问提供对用户私钥的访问。如前面所述，登录和口令访问通常不提供足够的安全性。

[0010] 用于增加上述密码系统的安全性的一种解决方案是包括生物测定作为验证或授权的一部分。生物测定一般包括可测量的物理特性，诸如例如，可由自动系统检查的指纹或语音，诸如例如，指纹模式或语音模式的模式匹配或识别。在这种系统中，用户的生物测定

和/或密钥可以存储在移动计算设备上，诸如例如，智能卡，膝上型电脑，个人数字助理或移动电话上，从而允许可以在移动环境中使用该生物测定或密钥。

[0011] 上述的移动生物测定密码系统仍然具有各种缺点。例如，移动用户可能丢失或损坏智能卡或便携计算设备，从而完全断绝他或她对潜在的重要数据的访问。可替换地，恶意人员可能偷窃移动用户的智能卡或便携计算设备，并且使用它有效地偷窃移动用户的数字凭证。在另一方面，便携计算设备可能被连接到开放系统，诸如Internet，并且类似于口令，存储着生物测定的文件很可能由于用户对安全性的粗心大意或恶意入侵者受到危及。

## 发明内容

[0012] 基于上述，存在提供安全性独立于用户同时仍然支持移动用户的密码系统的需要。

[0013] 因此本发明的一个方面是提供一种用于几乎保护任意类型数据不受未授权访问或使用的方法。该方法包括将要被保护的数据解析，分割和/或划分为两个或多个部件或部分的一个或多个步骤。该方法还包括对要被保护的数据加密。可以在数据的首次解析、分割和/或划分之前或之后执行数据加密。另外，可以针对数据的一个或多个部分重复加密步骤。类似地，可以为数据的一个或多个部分重复解析、分割和/或划分步骤。该方法可选择地还包括在一个位置或多个位置存储已被加密的解析、分割和/或划分的数据。该方法可选择地还包括为授权的访问或使用将受保护的数据重新构造或重新组装为其原始形式。该方法可被结合到能够执行该方法的所希望步骤的任意计算机、服务器、引擎等的操作中。

[0014] 本发明的另一个方面提供了一种用于几乎保护任意类型数据不受未授权访问或使用的系统。该系统包括数据分割模块，密码处理模块，和可选择地，数据组装模块。在一个实施例中，该系统还可以包括可以存储安全数据的一个或多个数据存储设备。

[0015] 因此本发明的一个方面是提供一种具有服务器中心密钥，或换言之在服务器上存储着密码密钥和用户验证数据的安全服务器或授信引擎。根据这个实施例，用户访问授信引擎以便执行验证和密码功能，诸如但不限于，例如，验证，授权，数字签名以及证书的产生、存储和检索，加密，公证类和委托类活动等。

[0016] 本发明的另一个方面是提供一种可靠的或可信的验证处理。另外，在可信赖的肯定验证之后，可以进行多种不同活动，从给系统或设备验证和访问提供密码技术，到允许使用或控制一种或多种电子设备。

[0017] 本发明的另一个方面是在密码密钥和验证数据不会丢失，被偷窃或受到危及的环境中提供密码密钥和验证数据，从而有利地避免了连续重发和管理新密钥和验证数据的需要。根据本发明的另一个方面，授信引擎允许用户针对多个活动、提供方和/或验证请求使用一个密钥对。根据本发明的另一个方面，授信引擎在服务器侧执行密码处理的至少一个步骤，诸如但不限于，加密，验证，或签名，从而允许客户或用户仅拥有最少的计算资源。

[0018] 根据本发明的另一个方面，授信引擎包括用于存储每个密码密钥和验证数据的多个部分的一个或多个仓库。通过数据分割处理创建这些部分，数据分割处理在没有来自一个仓库中的多于一个位置或来自多个仓库的预定部分的情况下禁止重新构造。根据另一个实施例，多个仓库在地理上可位于远方，从而无赖雇员或一个仓库处的受到危及的系统将不能提供对用户的密钥或验证数据的访问。

[0019] 根据另一个实施例，验证处理有利地允许授信引擎并行地处理多个验证活动。根据另一个实施例，授信引擎可以有利地追踪失败的访问尝试，并且从而限制恶意入侵者可以尝试破坏系统的次数。

[0020] 根据另一个实施例，授信引擎可以包括多个实例，其中每个授信引擎可以预测并且与其他授信引擎分摊处理负载。根据另一个实施例，授信引擎可以包括冗余模块，用于轮询多个验证结果以便确保多于一个系统验证用户。

[0021] 因此，本发明的一个方面包括可被远程访问的安全密码系统，其用于存储任意类型数据，包括但不限于将与多个用户相关联的多个私有密码密钥。该密码系统将多个用户中的每一个与所述多个私有密码密钥中的一个或多个不同密钥相关联，并且使用相关联的一个或多个不同密钥为每个用户执行密码功能，而不向用户发放多个私有密码密钥。该密码系统包括具有至少一个服务器的仓库系统，所述服务器存储将被保护的数据，诸如多个私有密码密钥和多个登记验证数据。每个登记验证数据标识多个用户中的一个，并且多个用户中的每一个用户与多个私有密码密钥中的一个或多个不同密钥相关联。该密码系统还可以包括验证引擎，其对通过多个用户中的一个用户接收的验证数据和从所述仓库系统接收的对应于多个用户中的这个用户的登记验证数据进行比较，从而产生验证结果。该密码系统还可以包括密码引擎，当验证结果指示对多个用户中的一个用户的正确识别时，密码引擎使用从仓库系统接收的相关联的一个或多个不同密钥代表多个用户中的这个用户执行密码功能。该密码系统还可以包括事务处理引擎，其连接为将来自多个用户的数据路由到仓库服务器系统、验证引擎和密码引擎。

[0022] 本发明的另一个方面包括一种可选择地可远程访问的安全密码系统。该密码系统包括具有至少一个服务器的仓库系统，所述服务器存储至少一个私钥和任意其他数据，诸如但不限于多个登记验证数据，其中每个登记验证数据标识可能的多个用户中的一个用户。该密码系统还可以可选择地包括验证引擎，其对通过用户接收的验证数据和从所述仓库系统接收的相应于该用户的登记验证数据进行比较，从而产生验证结果。该密码系统还包括密码引擎，当验证结果指示对用户的正确识别时，密码引擎使用可以从仓库系统接收的至少一个所述私钥代表该用户执行密码功能。该密码系统还可以可选择地包括事务处理引擎，其连接为将来自用户的数据路由到其他引擎或系统，诸如但不限于仓库服务器系统、验证引擎和密码引擎。

[0023] 本发明的另一个方面包括一种便于密码功能的方法。该方法包括将多个用户中的一个用户与存储在安全位置诸如安全服务器的多个私有密码密钥中的一个或多个密钥相关联。该方法还包括从用户处接收验证数据，并且对该验证数据和相应于该用户的验证数据进行比较，从而检验用户的身份。该方法还包括利用一个或多个密钥执行密码功能，而不向用户发放一个或多个密钥。

[0024] 本发明的另一个方面包括一种验证系统，其用于通过用户的登记验证数据的安全存储唯一地识别用户。该验证系统包括一个或多个数据存储设备，其中每个数据存储设备包括存储登记验证数据的至少一个部分的计算机可访问的存储介质。该验证系统还包括与该数据存储设备或多个设备通信的验证引擎。验证引擎包括数据分割模块，其对登记验证数据操作以便创建多个部分，数据组装模块，其处理来自至少一个数据存储设施的多个部分以便组装登记验证数据，和数据比较模块，其从用户处接收当前验证数据，并且对当前验

证数据和组装的验证数据进行比较以便确定用户是否被唯一地识别。

[0025] 本发明的另一个方面包括密码系统。该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存储一个或多个密码密钥的至少一个部分的计算机可访问的存储介质。该验证系统还包括与该数据存储设施通信的密码引擎。密码引擎还包括数据分割模块，其对密码密钥进行操作以便创建多个部分，数据组装模块，其处理来自至少一个数据存储设施的多个部分以便组装密码密钥，和密码处理模块，其接收组装的密码密钥并且以其执行密码功能。

[0026] 本发明的另一个方面包括一种存储任意类型数据的方法，所述数据包括但不限于地理上位于远方的安全数据存储实施内的验证数据，从而保护数据不受任何个人数据存储设施危及。该方法包括在授信引擎处接收数据，在授信引擎处将该数据和第一个基本上随机的数值组合以便形成第一组合值，并且将该数据和第二个基本上随机的数值组合以便形成第二组合值。该方法包括创建第一个基本上随机的数值和第二组合值的第一配对，创建第一个基本上随机的数值和第二个基本上随机的数值的第二配对，和在第一安全数据存储实施中存储第一配对。该方法包括在远离第一安全数据存储设施的第二安全数据存储设施中存储第二配对。

[0027] 本发明的另一个方面包括一种存储任意类型数据的方法，所述数据包括但不限于验证数据，该方法包括接收数据，将该数据和第一位集合组合以便形成第二位集合，和将该数据和第三位集合组合以便形成第四位集合。该方法还包括创建第一位集合和第三位集合的第一配对。该方法还包括创建第一位集合和第四位集合的第二配对，和在第一计算机可访问存储介质中存储第一和第二配对中的一个。该方法还包括在第二计算机可访问介质中存储第一和第二配对中的另一个。

[0028] 本发明的另一个方面包括在地理上位于远方的安全数据存储设备内存储密码数据，从而保护密码数据不受任何个人数据存储设施的危及的方法。该方法包括在授信引擎处接收密码数据，在授信引擎处将该密码数据和第一个基本上随机的数值组合以便形成第一组合值，以及将该密码数据和第二个基本上随机的数值组合以便形成第二组合值。该方法还包括创建第一个基本上随机的数值和第二组合值的第一配对，创建第一个基本上随机的数值和第二个基本上随机的数值的第二配对，和在第一安全数据存储实施中存储第一配对。该方法还包括在远离第一安全数据存储设施的第二安全数据存储设施中存储第二配对。

[0029] 本发明的另一个方面包括一种存储密码数据的方法，包括接收验证数据，和将密码数据和第一位集合组合以便形成第二位集合。该方法还包括将密码数据和第三位集合组合以便形成第四位集合，创建第一位集合和第三位集合的第一配对，和创建第一位集合和第四位集合的第二配对。该方法还包括在第一计算机可访问存储介质中存储第一和第二配对中的一个，并且在第二计算机可访问介质中存储第一和第二配对中的另一个。

[0030] 本发明的另一个方面包括处理密码系统中任意类型或形式的敏感数据的方法，其中所述敏感数据仅在被授权用户采用该敏感数据的活动期间以可用形式存在。该方法还包括在软件模块中从第一计算机可访问存储介质接收大体随机化或加密的敏感数据，并且在软件模块中从一个或多个其他计算机可访问存储介质接收可以是或可以不是敏感数据的大体随机化或加密的数据。该方法还包括在软件模块中处理该大体随机化或预加密的敏感

数据和可以是或可以不是敏感数据的大体随机化或加密的数据，以便组装该敏感数据并且在软件引擎中采用该敏感数据执行活动。该活动包括但不限于验证用户和执行密码功能中的一个。

[0031] 本发明的另一个方面包括一种安全验证系统。该安全验证系统包括多个验证引擎。每个验证引擎接收设计为以一种确定程度唯一标识用户的登记验证数据。每个验证引擎接收当前验证数据以便与登记验证数据进行比较，并且每个验证引擎确定一个验证结果。该安全验证系统还包括冗余系统，其接收至少两个验证引擎的验证结果，并且确定用户是否被唯一地识别。

[0032] 本发明的另一个方面包括一种运动中安全数据系统，从而数据可被以根据本发明受到保护的不同部分传输，从而被危及的任意一个部分不会提供足够的数据以便恢复原始数据。这可被应用于任意数据传输，不论是有线的、无线的还是物理的。

[0033] 本发明的另一个方面包括将本发明的安全数据解析器集成到存储或传递数据的任意适合的系统。例如，电子邮件系统，RAID 系统，视频广播系统，数据库系统，或可以在任意适合的级别集成安全数据解析器的任意其他适合的系统。

[0034] 本发明的另一个方面包括使用任意适合的解析和分割算法以产生数据的份。可以采用随机的算法、伪随机的算法、确定性的算法或其任意组合于解析和分割数据。

## 附图说明

[0035] 下面结合附图更详细地描述本发明，附图旨在说明而不是限制本发明，并且其中：

[0036] 图 1 示出了根据本发明的实施例的方面的密码系统的方框图；

[0037] 图 2 示出了根据本发明的实施例的方面的图 1 的授信引擎的方框图；

[0038] 图 3 示出了根据本发明的实施例的方面的图 2 的事务处理引擎的方框图；

[0039] 图 4 示出了根据本发明的实施例的方面的图 2 的仓库的方框图；

[0040] 图 5 示出了根据本发明的实施例的方面的图 2 的验证引擎的方框图；

[0041] 图 6 示出了根据本发明的实施例的方面的图 2 的密码引擎的方框图；

[0042] 图 7 示出了根据本发明的另一个实施例的方面的仓库系统的方框图；

[0043] 图 8 示出了根据本发明的实施例的方面的数据分割处理的流程图；

[0044] 图 9，版面 A 示出了根据本发明的实施例的方面的登记处理的数据流；

[0045] 图 9，版面 B 示出了根据本发明的实施例的方面的互操作性处理的流程图；

[0046] 图 10 示出了根据本发明的实施例的方面的验证处理的数据流；

[0047] 图 11 示出了根据本发明的实施例的方面的签署处理的数据流；

[0048] 图 12 示出了根据本发明的另一个实施例的方面的加密 / 解密处理的数据流；

[0049] 图 13 示出了根据本发明的另一个实施例的方面的授信引擎系统的简化方框图；

[0050] 图 14 示出了根据本发明的另一个实施例的方面的授信引擎系统的简化方框图；

[0051] 图 15 示出了根据本发明的实施例的方面的图 14 的冗余模块的方框图；

[0052] 图 16 示出了根据本发明的一个方面的用于评估验证的处理；

[0053] 图 17 示出了根据本发明图 16 所示的一个方面的用于给验证分配值的处理；

[0054] 图 18 示出了图 17 所示的本发明一个方面中的用于执行信任仲裁的处理；

[0055] 图 19 示出了根据本发明的实施例的方面的用户和提供方之间的示例事务处理，其中初始的基于 Web 的接触导致双方签署的销售合同；

[0056] 图 20 示出了具有给用户系统提供安全功能的密码服务提供商模块的示例用户系统；

[0057] 图 21 示出了具有加密和加密主密钥与数据的存储的用于解析、分割和 / 或划分数据的处理；

[0058] 图 22 示出了具有加密和加密主密钥与数据的分离存储的用于解析、分割和 / 或划分数据的处理；

[0059] 图 23 示出了具有加密和加密主密钥与数据的存储的用于解析、分割和 / 或划分数据的中间密钥处理；

[0060] 图 24 示出了具有加密和加密主密钥与数据的分离存储的用于解析、分割和 / 或划分数据的中间密钥处理；

[0061] 图 25 以小的工作组示出了对本发明的密码方法和系统的利用；

[0062] 图 26 是根据本发明的一个实施例的采用安全数据解析器的说明性物理标记安全系统的方框图；

[0063] 图 27 是一种说明性布置的方框图，其中根据本发明的一个实施例，将安全数据解析器集成到一个系统内；

[0064] 图 28 是根据本发明的一个实施例的说明性运动中数据系统的方框图；

[0065] 图 29 是根据本发明的一个实施例的另一个说明性运动中数据系统的方框图；

[0066] 图 30-32 是根据本发明的一个实施例集成有安全数据解析器的说明性系统的方框图；

[0067] 图 33 是根据本发明的一个实施例的用于解析和分割数据的说明性处理的处理流图示；

[0068] 图 34 是根据本发明的一个实施例的用于将数据的多个部分恢复为原始数据的说明性处理的处理流图示；

[0069] 图 35 是根据本发明的一个实施例的用于在位级别分割数据的说明性处理的处理流图示；

[0070] 图 36 是根据本发明的一个实施例，可被以任意适合的添加、删除或修改按任意适合的组合使用的说明性步骤和特征的处理流图示；

[0071] 图 37 是根据本发明的一个实施例，可被以任意适合的添加、删除或修改按任意适合的组合使用的说明性步骤和特征的处理流图示；

[0072] 图 38 是根据本发明的一个实施例，可被以任意适合的添加、删除或修改按任意适合的组合使用的份中的密钥和数据组件的存储的简化方框图；

[0073] 图 39 是根据本发明的一个实施例，可被以任意适合的添加、删除或修改按任意适合的组合使用的，使用工作组密钥的份中的密钥和数据组件的存储的简化方框图；

[0074] 图 40A 和 40B 是根据本发明的一个实施例，可被以任意适合的添加、删除或修改按任意适合的组合使用的包头产生和运动中数据的数据分割的简化和说明性处理流图示；

[0075] 图 41 是根据本发明的一个实施例，可被以任意适合的添加、删除或修改按任意适合的组合使用的说明性份格式的简化方框图。

## 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一个授信引擎存储密码密钥和用户验证数据。用户通过对授信引擎的网络访问访问常规密码系统的功能，然而，授信引擎不发放实际密钥和其他验证数据，并且因此密钥和数据保持为是安全的。密钥和验证数据的这个服务器中心存储提供了独立于用户的安全性、便携性、可用性和直观性。

[0077] 由于用户可以信任或信赖密码系统执行用户和文档验证和其他密码功能，各种功能可被结合到该系统内。例如，授信引擎提供商可以通过例如验证协议参与人，代表或为参与人数字签署协议，并且存储由每个参与人数字签署的协议的记录，确保防止协议抵赖。另外，密码系统可以监视协议，并且基于例如价格，用户，提供方，地理位置，使用位置等确定应用不同程度的验证。

[0078] 为了便于完整理解本发明，详细描述的剩余部分参考附图描述本发明，其中通篇以类似的数字指示类似的元件。

[0079] 图 1 示出了根据本发明的实施例的方面的密码系统 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，证书颁发机构 115 和提供方系统 120。

[0080] 根据本发明的一个实施例，用户系统 105 包括具有一个或多个微处理器诸如例如基于 Intel 的处理器的常规通用计算机。另外，用户系统 105 包括适当的操作系统，诸如例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 可以包括生物测定设备 107。生物测定设备 107 可以有利地捕捉用户的生物测定，并且将捕捉的生物测定传输到授信引擎 110。根据本发明的一个实施例，生物测定设备可以有利地包括具有类似于提交于 1997 年 9 月 5 日的题目为" RELIEF OBJECT IMAGE GENERATOR" 的美国专利申请 No. 08/926,277，提交于 2000 年 4 月 26 日的题目为" IMAGING DEVICE FOR A RELIEF OBJECT AND SYSTEM AND METHOD OF USING THE IMAGE DEVICE" 的美国专利申请 No. 09/558,634，提交于 1999 年 11 月 5 日的题目为" RELIEF OBJECT SENSOR ADAPTOR" 的美国专利申请 No. 09/435,011 和提交于 2000 年 1 月 5 日的题目为" PLANAR OPTICAL IMAGE SENSOR AND SYSTEM FOR GENERATING AN ELECTRONIC IMAGE OF A RELIEF OBJECT FOR FINGERPRINT READING" 的美国专利申请 No. 09/477,943 中公开的属性和特征的设备，所有这些为当前受让人所有，并且这里引用所有这些作为参考。

[0081] 另外，用户系统 105 可以通过常规的服务提供商，诸如例如拨号，数字用户线路 (DSL)，缆线调制解调器，光纤连接等连接到通信链路 125。根据另一个实施例，用户系统 105 通过网络连接，诸如例如，局域网或广域网连接通信链路 125。根据一个实施例，操作系统包括处理经过通信链路 125 的所有进入和外出消息流的 TCP/IP 栈。

[0082] 虽然参考前面的实施例公开了用户系统 105，本发明不旨在局限于此。而是本领域的技术人员从此处的公开中将会认识到用户系统 105 的多种替代实施例，包括能够从另一个计算机系统发送或接收信息的几乎任意计算设备。例如，用户系统 105 可以包括但不限于可以与通信链路 125 交互的计算机工作站，交互电视，交互信息亭，诸如数字助理，移动电话，膝上计算机等的个人移动计算设备，无线通信设备，智能卡，嵌入计算设备等。在这些

可替换系统中，操作系统很可能不同，并且适合于特定的设备。然而，根据一个实施例，操作系统有利地继续提供建立与通信链路 125 的通信所需的适当通信协议。

[0083] 图 1 示出了授信引擎 110。根据一个实施例，授信引擎 110 包括用于访问和存储敏感信息的一个或多个安全服务器，敏感信息可以是任意类型或形式的数据，诸如但不限于文本，音频，视频，用户验证数据和公共和私有密码密钥。根据一个实施例，验证数据包括设计为唯一标识密码系统 100 的用户的数据。例如，验证数据可以包括用户识别码，一个或多个生物测定，和由授信引擎 110 或用户产生但是最初由用户在登记时回答的一系列问题和答案。上述问题可以包括人口统计数据，诸如出生地，地址，周年纪念等；个人数据，诸如妈妈的婚前姓名，最喜欢的冰淇淋等，或设计为唯一标识用户的其他数据。授信引擎 110 对与当前事务处理相关联的用户验证数据和以前诸如在登记过程中提供的验证数据进行比较。授信引擎 110 可以有利地请求用户在每次事务处理时产生验证数据，或授信引擎 110 可以有利地允许用户周期地产生验证数据，诸如在一连串事务处理的开始时或登录到特定提供方的 Web 站点时。

[0084] 根据用户产生生物测定数据的实施例，用户给生物测定设备 107 提供物理特性，诸如但不限于，脸部扫描，手扫描，耳扫描，虹膜扫描，视网膜扫描，血管模式，DNA，指纹，笔迹或语音。生物测定设备有利地产生物理特性的电子模式或生物测定。所述电子模式被出于登记或验证目的通过用户系统 105 传输到授信引擎 110。

[0085] 一旦用户产生了适当的验证数据，并且授信引擎 110 确定验证数据（当前验证数据）和登记时提供的验证数据（登记验证数据）之间的肯定匹配，授信引擎 110 给用户提供完整的密码功能。例如，正确验证的用户可以有利地采用授信引擎 110 执行散列，数字签名，加密和解密（通常仅被一块称为加密），创建或分发数字证书等。然而，在授信引擎 110 之外不可获得密码功能中使用的私有密码密钥，从而确保了密码密钥的完整性。

[0086] 根据一个实施例，授信引擎 110 产生并且存储密码密钥。根据另一个实施例，至少一个密码密钥被与每个用户相关联。另外，当密码密钥包括公钥技术时，在其中产生与用户相关联的每个私钥，并且不从授信引擎 110 发放私钥。因此只要用户能够访问授信引擎 110，用户可以使用他或她的私钥或公钥执行密码功能。这种远程访问有利地允许用户保持完全的移动性，并且通过几乎任意 Internet 连接诸如蜂窝和卫星电话，信息亭，膝上计算机，旅馆房间访问密码功能。

[0087] 根据另一个实施例，授信引擎 110 使用为授信引擎 110 产生的密钥对执行密码功能。根据这个实施例，授信引擎 110 首先验证用户，并且在用户已经正确产生与登记验证数据匹配的验证数据之后，授信引擎 110 使用它自己的密码密钥对代表被验证的用户执行密码功能。

[0088] 本领域的技术人员将从此处的公开中认识到密码密钥可以有利地包括对称密钥，公钥和私钥中的某些或全部。另外，本领域的技术人员将从此处的公开中认识到，可以使用可以根据商业技术获得的各种算法实现上述密钥，诸如例如 RSA，ELGAMAL 等。

[0089] 图 1 还示出了证书颁发机构 115。根据一个实施例，证书颁发机构 115 可以有利地包括颁发数字证书的可信任的第三方组织或公司，诸如例如，Verisign，Baltimore，Entrust 等。授信引擎 110 可以有利地通过一个或多个常规数字证书协议，诸如例如，PKCS10 向证书颁发机构 115 传输对数字证书的请求。作为响应，证书颁发机构 115 将以若

干不同协议中的一个或多个例如 PKCS7 颁发数字证书。根据一个实施例，授信引擎 110 从若干或全部著名证书颁发机构 115 请求数字证书，从而授信引擎 110 可以访问相应于任意请求方的证书标准的数字证书。

[0090] 根据另一个实施例，授信引擎 110 内部地执行证书颁发。在这个实施例中，授信引擎 110 可以访问证书系统以便产生证书，和 / 或可以在请求证书时，诸如例如，在密钥产生时，或以请求时被请求的证书标准中内部地产生证书。将在下面更详细地公开授信引擎 110。

[0091] 图 1 还示出了提供方系统 120。根据一个实施例，提供方系统 120 有利地包括 Web 服务器。典型的 Web 服务器使用若干 Internet 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) 中的一种在 Internet 上提供内容服务。Web 服务器从例如 Netscape 和 Internet Explorer 的浏览器接受请求，然后返回适当的电子文档。可以使用若干服务器或客户机侧技术提升 Web 服务器的能力，使得超出其传递标准电子文档的能力。例如，这些技术包括公共网关接口 (CGI) 脚本，安全套接字层 (SSL) 安全性和活动服务器页面 (ASP)。提供方系统 120 可以有利地提供关于商业，个人，教育或其他事务处理的电子内容。

[0092] 虽然参考上面的实施例公开了提供方系统 120，本发明不旨在局限于此。而是本领域的技术人员将从此处的公开中认识到，提供方系统 120 可以有利地包括参考用户系统 105 或其组合描述的任意设备。

[0093] 图 1 还示出了连接用户系统 105，授信引擎 110，证书颁发机构 115 和提供方系统 120 的通信链路 125。根据一个实施例，通信链路 125 优选地包括 Internet。如在本公开中通篇使用的，Internet 是计算机的全球网络。本领域的技术人员所公知的 Internet 的结构包括网络主干，从主干分支出的网络。这些分支又具有从它们分支出的网络等等。路由器在网络层之间，然后在网络间移动信息包，直到该包到达其目的地附近为止。从目的地出发，目的地网络的主机将信息包发送到适当的终端或节点。在一个有利的实施例中，如本领域所公知的，Internet 路由集线器包括使用传输控制协议 / 网际协议 (TCP/IP) 的域名系统 (DNS) 服务器。路由集线器通过高速通信链路连接到一个或多个其他路由集线器。

[0094] Internet 的一个流行部分是万维网。万维网包括存储着能够显示图形和文本信息的文档的不同计算机。在万维网上提供信息的计算机通常被称为“Web 站点”。以具有相关联的电子页面的 Internet 地址定义 Web 站点。可由统一资源定位器 (URL) 标识电子页面。一般地，电子页面是以组织文本、图形图像、音频、视频等形式呈现的文档。

[0095] 虽然以其优选实施例的方式公开了通信链路 125，本领域的普通技术人员将从此处的公开中认识到通信链路 125 可以包括各种交互通信链路。例如，通信链路 125 可以包括交互电视网络，电话网络，无线数据传输系统，双路电缆系统，定制的私有或公有计算机网络，交互式信息亭网络，自动应答机网络，直接链路，卫星或蜂窝网络等。

[0096] 图 2 示出了根据本发明的实施例的方面的图 1 的授信引擎 110 的方框图。如图 2 所示，授信引擎 110 包括事务处理引擎 205，仓库 210，验证引擎 215 和密码引擎 220。根据本发明的一个实施例，授信引擎 110 还包括海量存储器 225。如图 2 进一步所示，事务处理引擎 205 与仓库 210、验证引擎 215 和密码引擎 220 以及海量存储器 225 通信。另外，仓库 210 与验证引擎 215，密码引擎 220 和海量存储器 225 通信。另外，验证引擎 215 与密码引

擎 220 通信。根据本发明的一个实施例，上述通信中的某些或全部可以有利地包括 XML 文档到相应于接收设备的 IP 地址的传输。如前所述，XML 文档有利地允许设计者创建自己所有的定制文档标签，使得能够进行应用间和组织间的数据定义、传输、验证和说明。另外，上述通信中的某些或全部可以包括常规 SSL 技术。

[0097] 根据一个实施例，事务处理引擎 205 包括数据路由设备，诸如可以从 Netscape，Microsoft，Apache 等获得的常规 Web 服务器。例如，Web 服务器可以有利地接收来自通信链路 125 的进入数据。根据本发明的一个实施例，该进入数据被寻址到用于授信引擎 110 的前端安全系统。例如，该前端安全系统可以有利地包括防火墙，搜索已知攻击简档的入侵检测系统和 / 或病毒扫描器。在穿过前端安全系统之后，数据被事务处理引擎 205 接收并且被路由到仓库 210，验证引擎 215，密码引擎 220 和海量存储器 225 之一。另外，事务处理引擎 205 监视来自验证引擎 215 和密码引擎 220 的进入数据，并且通过通信链路 125 将数据路由到特定系统。例如，事务处理引擎 205 可以有利地将数据路由到用户系统 105、证书颁发机构 115 或提供方系统 120。

[0098] 根据一个实施例，使用常规的 HTTP 路由技术，诸如例如采用 URL 或统一资源指示符 (URI) 路由数据。URI 类似于 URL，然而 URI 通常指示文件或动作的来源，例如可执行、脚本等等。因此，根据一个实施例，用户系统 105、证书颁发机构 115、提供方系统 120 和授信引擎 210 的组件有利地在事务处理引擎 205 的通信 URL 或 URI 内包括足够的数据，以便在密码系统中正确地路由数据。

[0099] 虽然参考其优选实施例公开了数据路由，本领域的技术人员将认识到各种可能的路由方案或策略。例如，可以有利地根据其格式、内容等解包和识别 XML 或其他数据包，从而事务处理引擎 205 可以正确地在授信引擎 110 中路由数据。另外，本领域的技术人员将认识到，诸如例如，当通信链路 125 包括局域网时，可以有利地使得数据路由适合于符合特定网络系统的数据传输协议。

[0100] 根据本发明的另一个实施例，事务处理引擎 205 包括常规的 SSL 加密技术，从而在特定通信中，上述系统可以使用事务处理引擎 205 验证自身，并且反之亦然。如在本公开中使用的，术语“1/2 SSL”指服务器是 SSL 验证的而客户机不必如此的通信，并且术语“全 SSL”指客户机和服务器为 SSL 验证的通信。当本公开使用术语“SSL”时，通信可以包括 1/2 或全 SSL。

[0101] 当事务处理引擎 205 将数据路由到密码系统 100 的各种组件时，事务处理引擎 205 可以有利地创建审查线索。根据一个实施例，审查线索包括至少事务处理引擎 205 路由到密码系统 100 各处的数据的类型和格式的记录。这种审查数据可被有利地存储在海量存储器 225 内。

[0102] 图 2 还示出了仓库 210。根据一个实施例，仓库 210 包括一个或多个数据存储设施，诸如例如，目录服务器，数据库服务器等。如图 2 所示，仓库 210 存储密码密钥和登记验证数据。密码密钥可以有利地对应于授信引擎 110 或对应于密码系统 100 的用户，诸如用户或提供方。登记验证数据可以有利地包括设计为唯一地标识用户的数据，诸如用户 ID，口令，对问题的回答，生物测定数据等。可以在用户登记时或在另一个可供选择的稍后时间有利地获取登记验证数据。例如，授信引擎 110 可以包括登记验证数据的周期或其他形式的更新或重发。

[0103] 根据一个实施例，从事务处理引擎 205 到验证引擎 215 和密码引擎 220 以及从验证引擎 215 和密码引擎 220 到事务处理引擎 205 的通信包括安全通信，诸如例如，常规的 SSL 技术。另外，如前所述，到和来自仓库 210 的通信的数据可被使用 URL，URI，HTTP，或 XML 文档传输，其中在上述任意一个中有利地嵌入数据请求和格式。

[0104] 如上所述，仓库 210 可以有利地包括多个安全数据存储设施。在这样一个实施例中，可以这样配置安全数据存储设施，从而对一个单独数据存储设施的安全的危及不会危及存储在其中的密码密钥或验证数据。例如，根据这个实施例，对密码密钥和验证数据进行数学操作，以便统计地并且充分地随机化存储在单个数据存储设施内的数据。根据一个实施例，单个数据存储设施的数据的随机化致使数据不可译码。因此，对单个数据存储设施的危及仅产生随机化的不可译码的数字，并且整体上不会危及任意密码密钥或验证数据的安全性。

[0105] 图 2 还示出了包括验证引擎 215 的授信引擎 110。根据一个实施例，验证引擎 215 包括配置为对来自事务处理引擎 205 的数据和来自仓库 210 的数据进行比较的数据比较器。例如，在验证过程中，用户将当前验证数据提供给授信引擎 110，从而事务处理引擎 205 接收当前验证数据。如前所述，事务处理引擎 205 优选地识别 URL 或 URI 中的数据请求，并且将验证数据路由到验证引擎 215。另外，依据请求，仓库 210 将相应于该用户的登记验证数据转发到验证引擎 215。因此，验证引擎 215 具有当前验证数据和登记验证数据两者以便进行比较。

[0106] 根据一个实施例，到验证引擎的通信包括安全通信，诸如例如，SSL 技术。附加地，可以在授信引擎 110 组件内提供安全性，诸如例如，使用公钥技术的超级加密。例如，根据一个实施例，用户以验证引擎 215 的公钥对当前验证数据加密。另外，仓库 210 还以验证引擎 215 的公钥对登记验证数据加密。以这种方式，仅可以使用验证引擎的私钥对传输进行解密。

[0107] 如图 2 所示，授信引擎 110 还包括密码引擎 220。根据一个实施例，密码引擎包括密码处理模块，其被有利地配置为提供常规密码功能，诸如例如，公钥基础设施 (PKI) 功能。例如，密码引擎 220 可以有利地为密码系统 100 的用户颁发公钥和私钥。以这种方式，密码密钥被在密码引擎 220 处产生并且被转发到仓库 210，从而在授信引擎 110 之外至少不可获得私有密码密钥。根据另一个实施例，密码引擎 220 随机化并且分割至少私有密码密钥数据，从而仅存储随机化的分割数据。类似于登记验证数据的分割，分割处理确保在密码引擎 220 之外不可获得存储的密钥。根据另一个实施例，密码引擎的功能可被与验证引擎 215 组合并且由验证引擎 215 执行。

[0108] 根据一个实施例，到和来自密码引擎的通信包括安全通信，诸如 SSL 技术。另外，可以有利地采用 XML 文档传输数据和 / 或进行密码功能请求。

[0109] 图 2 还示出了具有海量存储器 225 的授信引擎 110。如前所述，事务处理引擎 205 保持相应于审查线索的数据，并且在海量存储器 225 中存储这种数据。类似地，根据本发明的一个实施例，仓库 210 保持相应于审查线索的数据，并且在海量存储器 225 中存储这种数据。仓库审查线索数据类似于事务处理引擎 205 的审查线索数据，因为审查线索数据包括仓库 210 接收的请求和对其的响应的记录。另外，海量存储器 225 可用于存储其中包含用户的公钥的数字证书。

[0110] 虽然参考其优选和可替换实施例公开了授信引擎110，本发明不旨在局限于此。而是本领域的技术人员将认识到此处公开的授信引擎 110 的多种替换方案。例如，授信引擎 110 可以有利地仅执行验证，或可替换地仅执行密码功能中的某些或全部，诸如数据加密和解密。根据这种实施例，可以有利地去除验证引擎 215 和密码引擎 220 之一，从而创建授信引擎 110 的更直观的设计。另外，密码引擎 220 还可以与证书颁发机构通信，从而将证书颁发机构包含在授信引擎 110 内。根据另一个实施例，授信引擎 110 可以有利地执行验证和一个或多个密码功能，诸如例如，数字签名。

[0111] 图 3 示出了根据本发明的实施例的方面的图 2 的事务处理引擎 205 的方块图。根据这个实施例，事务处理引擎 205 包括具有处理线程和侦听线程的操作系统 305。操作系统 305 可以有利地类似于常规大容量服务器，诸如例如，可从 Apache 获得的 Web 服务器中所常见的操作系统。侦听线程监视来自通信链路 125，验证引擎 215 和密码引擎 220 之一的进入通信的进入数据流。处理线程识别进入数据流的特定数据结构，诸如例如，前述的数据结构，从而将进入数据路由到通信链路 125、仓库 210、验证引擎 215、密码引擎 220 或海量存储 225 之一。如图 3 所示，可以有利地通过例如 SSL 技术保护进入和外出数据。

[0112] 图 4 示出了根据本发明的实施例的方面的图 2 的仓库 210 的方块图。根据这个实施例，仓库 210 包括一个或多个轻量级目录访问协议 (LDAP) 服务器。可以从各种制造商诸如 Netscape，ISO 等制造商获得 LDAP 目录服务器。图 4 还示出目录服务器优选地存储相应于密码密钥的数据 405 和相应于登记验证数据的数据 410。根据一个实施例，仓库 210 包括将验证数据和密码密钥数据索引到唯一用户 ID 的单个逻辑存储器结构。该单个逻辑存储器结构优选地包括存储在其内的数据的高度可信或高度安全的机制。例如，仓库 210 的物理位置有利地包括各种常规安全措施，诸如受限的雇员访问，调制解调器监视系统等。除了物理安全之外或取代物理安全，计算机系统或服务器可以有利地包括保护存储的数据的软件解决方案。例如，仓库 210 可以有利地创建和存储相应于采取的活动的审查线索的数据 415。另外，可以有利地以与常规 SSL 技术耦合的公钥加密对进入和外出通信加密。

[0113] 根据另一个实施例，如参考图 7 进一步公开的，仓库 210 可以包括不同的并且物理分离的数据存储设施。

[0114] 图 5 示出了根据本发明的实施例的方面的图 2 的验证引擎 215 的方块图。类似于图 3 的事务处理引擎 205，验证引擎 215 包括至少具有常规 Web 服务器，诸如例如，可从 Apache 获得的 Web 服务器的修改版本的侦听和处理线程的操作系统 505。如图 5 所示，验证引擎 215 包括到至少一个私钥 510 的访问。可以有利地使用私钥 510 例如对来自事务处理引擎 205 或仓库 210 的被以验证引擎 215 的相应公钥加密的数据解密。

[0115] 图 5 还示出了包括比较器 515、数据分割模块 520 和数据组装模块 525 的验证引擎 215。根据本发明的优选实施例，比较器 515 包括能够比较关于上述生物测定验证数据的潜在复杂模式的技术。该技术可以包括硬件、软件或用于模式比较的组合解决方案，诸如例如，表示指纹模式或语音模式的那些模式比较。另外，根据一个实施例，验证引擎 215 的比较器 515 可以有利地比较文档的常规散列，以便生成比较结果。根据本发明的一个实施例，比较器 515 包括将启发 530 应用于比较。启发 530 可以有利地解决围绕验证尝试的各种环境，诸如例如，一天中的时间、IP 地址或子网掩码、购买简档、电子邮件地址、处理器序列号或 ID 等。

[0116] 另外，生物测定数据比较的特性可能导致根据当前生物测定验证数据和登记数据的匹配产生的不同置信程度。例如，不同于仅可以返回肯定或否定匹配的传统口令，指纹可被确定为部分匹配，例如，90％匹配，75％匹配或10％匹配，而不是简单地正确或不正确。其他生物测定标识符，诸如声纹分析或面部识别可以分担概率验证而不是绝对验证的这种属性。

[0117] 当以这种概率验证工作，或在验证被认为不绝对可靠的其他情况下，希望应用启发530确定验证中提供的置信级别是否足够高到验证正在进行的事务处理。

[0118] 某些时候，待解决的事务处理是可以在较低置信级别被接受为通过验证的相对低价值的事务处理。这可以包括具有与其相关联的低货币价值（例如，$10的购买）的事务处理或低风险的事务处理（例如，允许进入仅对成员开放的Web站点）。

[0119] 相反，对于其他事务处理的验证，可能希望在允许进行事务处理之前需要高的验证置信程度。这种事务处理可以包括大货币价值（例如，签署几百万美元的供应合同）的事务处理，或如果发生不正确的验证的具有高风险的事务处理（例如，远程登录政府计算机）。

[0120] 可以如下所述那样结合置信级别和事务处理价值使用启发530，以便允许比较器提供动态的上下文敏感的验证系统。

[0121] 根据本发明的另一个实施例，比较器515可以有利地追踪特定事务处理的验证尝试。例如，当事务处理失败时，授信引擎110可以请求用户重新输入他或她的当前验证数据。验证引擎215的比较器515可以有利地采用尝试限制器535限制验证尝试的次数，从而阻止模仿用户的验证数据的暴力尝试。根据一个实施例，尝试限制器535包括监视事务处理的重复验证尝试，并且例如将给定事务处理的验证尝试限制为3次的软件模块。因此，尝试限制器535将模仿个人的验证数据的自动尝试限制为例如仅为3次“猜测”。在3次失败之后，尝试限制器535可以有利地拒绝附加的验证尝试。可以有利地通过例如不论正被传输的当前验证数据如何，比较器515返回否定结果来实现这种拒绝。在另一方面，事务处理引擎205可以有利地阻塞属于其中以前3次尝试已经失败的事务处理的任意附加验证尝试。

[0122] 验证引擎215还包括数据分割模块520和数据组装模块525。数据分割模块520有利地包括具有对各种数据进行数学操作，以便充分随机化数据并且将其分割为多个部分的能力的软件，硬件或组合模块。根据一个实施例，不能根据单个部分创建原始数据。数据组装模块525有利地包括配置为对上述充分随机化的部分进行数学操作，从而使其组合提供原始译码数据的软件，硬件或组合模块。根据一个实施例，验证引擎215采用数据分割模块520随机化登记验证数据并且将其分割为多个部分，并且采用数据组装模块525将这些部分重新组装为可以使用的登记验证数据。

[0123] 图6示出了根据本发明的一个实施例的方面的图2的授信引擎200的密码引擎220的方框图。类似于图3的事务处理引擎205，密码引擎220包括至少具有诸如例如可从Apache获得的Web服务器的常规Web服务器的修改版本的处理和侦听线程的操作系统605。如图6所示，密码引擎220包括具有类似于图5的那些功能的数据分割模块610和数据组装模块620。然而根据一个实施例，与前面的登记验证数据相反，数据分割模块610和数据组装模块620处理密码密钥数据。虽然，本领域的技术人员将从此处的公开中认识到，

数据分割模块610和数据组装模块620可与验证引擎215的那些数据分割模块和数据组装组合在一起。

[0124] 密码引擎220还包括配置为执行多个密码功能中的一种、某些或全部的密码处理模块625。根据一个实施例，密码处理模块625可以包括软件模块或程序、硬件，或这两者。根据另一个实施例，密码处理模块625可以执行数据比较，数据解析，数据分割，数据划分，数据散列，数据加密或解密，数字签名检验或创建，数字证书产生、存储或请求，密码密钥生成等。另外，本领域的技术人员将从此处的公开中认识到，密码处理模块625可以有利地包括公钥基础设施，诸如Pretty Good Privacy(PGP)，基于RSA的公钥系统，或各种可替换的密钥管理系统。另外，密码处理模块625可以执行公钥加密，对称密钥加密或这两者。除了前述之外，密码处理模块625可以包括一个或多个用于实现无缝的透明的互操作性功能的计算机程序或模块、硬件，或这两者。

[0125] 本领域的技术人员将从此处的公开中认识到，密码功能可以包括通常涉及密码密钥管理系统的多种或各种功能。

[0126] 图7示出了根据本发明的实施例的几方面的仓库系统700的简化方框图。如图7所示，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，本领域的普通技术人员容易理解，该仓库系统可以仅具有一个数据存储设施。根据本发明的一个实施例，数据存储设施D1到D4中的每一个可以有利地包括根据图4的仓库210公开的元件中的某些或全部。类似于仓库210，数据存储设施D1到D4优选地通过常规的SSL与事务处理引擎205，验证引擎215，密码引擎220通信。传输例如XML文档的通信链路。来自事务处理引擎205的通信有利地包括对数据的请求，其中该请求被有利地广播到每个数据存储设施D1到D4的IP地址。在另一方面，事务处理引擎205可以基于许多标准，诸如例如，响应时间，服务器负载，维护调度等将请求广播到特定的数据存储设施。

[0127] 响应来自事务处理引擎205的对数据的请求，仓库系统700有利地将存储的数据转发到验证引擎215和密码引擎220。相应的数据组装模块接收转发的数据，并且将数据组装为可用格式。在另一方面，从验证引擎215和密码引擎220到数据存储设施D1到D4的通信可以包括将被存储的敏感数据的传输。例如，根据一个实施例，验证引擎215和密码引擎220可以有利地采用其各自的数据分割模块将敏感数据划分为不可译码的部分，然后将敏感数据的一个或多个不可译码的部分传输到特定的数据存储设施。

[0128] 根据一个实施例，每个数据存储设施D1到D4包括单独的并且独立存储系统，诸如例如，目录服务器。根据本发明的另一个实施例，仓库系统700包括多个地理上分离的独立数据存储系统。通过将敏感数据分散到不同的并且独立的存储实施D1到D4，存储实施D1到D4中的某些或全部可以有利地在地理上分离，除了附加的安全措施之外，仓库系统700提供了冗余性。例如，根据一个实施例，仅需要来自多个数据存储设施D1到D4中的两个数据存储设施的数据来译码并且重新组装敏感数据。因此，四个数据存储设施D1到D4中的多至两个数据存储设施可能由于维护，系统故障，电源故障等而不可操作，而不会影响授信引擎110的功能。另外，根据一个实施例，由于存储在每个数据存储设施内的数据被随机化并且是不可译码的，对任意单独数据存储设施的危及不必然危及该敏感数据。另外，在具有地理分离的数据存储设施的实施例中，危及多个在地理上位于远方的设施变得更加困难。事实上，甚至诈骗雇员破坏所需的多个独立的地理上位于远方的数据存储设施也是极具挑战

性的。

[0129] 虽然参考其优选和可替换的实施例公开了仓库系统 700，本发明不旨在局限于此。而是本领域的技术人员将从此处的公开中认识到仓库系统 700 的许多替代方案。例如，仓库系统 700 可以包括一个或两个或多个数据存储设施。另外，可以数学地操作敏感数据，从而需要来自两个或多个数据存储设施的部分以便重新组装并且译码敏感数据。

[0130] 如前所述，验证引擎 215 和密码引擎 220 中的每一个分别包括用于分割任意类型或形式的敏感数据，诸如例如，文本、音频、视频、验证数据和密码密钥数据的数据分割模块 520 和 610。图 8 示出了根据本发明的实施例的方面由数据分割模块执行的数据分割处理 800 的流程图。如图 8 所示，当验证引擎 215 或密码引擎 220 的数据分割模块接收到敏感数据“S”时，数据分割处理 800 以步骤 805 开始。优选地，在步骤 810，数据分割模块然后产生大体随机的数字、值或串或位集合“A”。例如，可以根据本领域普通技术人员可使用的用于产生适合于在密码应用中使用的高质量随机数的许多不同常规技术产生随机数 A。另外，根据一个实施例，随机数 A 包括可以是任意适合长度的位长度，诸如比敏感数据 S 的位长度更短、更长或相等。

[0131] 另外，在步骤 820，数据分割处理 800 产生另一个统计上随机的数字“C”。根据优选实施例，可以有利地并行完成统计上随机的数字 A 和 C 的产生。然后数据分割模块将数字 A 和 C 与敏感数据 S 组合，从而产生新数字“B”和“D”。例如，数字 B 可以包括 A XOR S 的二进制组合，并且数字 D 可以包括 C XOR S 的二进制组合。XOR 函数或“异或”函数是本领域的技术人员公知的。上述组合优选地分别发生在步骤 825 和 830，并且根据一个实施例，上述组合还可以并行发生。数据分割处理 800 然后进入步骤 835，其中配对随机数 A 和 C 以及数字 B 和 D，从而没有一个配对自身包含足够的数据以便重新组装和译码原始敏感数据 S。例如，数字可被如下配对 :AC，AD，BC 和 BD。根据一个实施例，上述配对中的每一个被分配到图 7 的仓库 D1 到 D4 中的一个。根据另一个实施例，上述配对中的每一个被随机地分配到仓库 D1 到 D4 中的一个。例如，在第一数据分割处理 800 过程中，配对 AC 可被通过例如对 D2 的 IP 地址的随机选择发送到仓库 D2。然后，在第二数据分割处理 800 过程中，配对 AC 可被通过例如对 D4 的 IP 地址的随机选择发送到仓库 D4。另外，配对可被全部存储在一个仓库上，并且可被存储在所述仓库上的分离的位置内。

[0132] 基于上文，数据分割处理 800 有利地将敏感数据的多个部分放置在 4 个数据存储设施 D1 到 D4 中的每一个内，从而没有单个数据存储设施 D1 到 D4 包括足够的加密数据以便重建原始敏感数据 S。如前所述，这种将数据随机化为不可单独使用的加密部分增加了安全性，并且即使数据存储设施 D1 到 D4 中的一个受到危及，也可提供数据的持续可信。

[0133] 虽然参考其优选实施例公开了数据分割处理 800，本发明不旨在局限于此。而是本领域的技术人员将从此处的公开中认识到数据分割处理 800 的各种替代方案。例如，数据分割处理可以有利地将数据分割为两个数字，例如随机数字 A 和数字 B，并且随机地通过两个数据存储设施分配 A 和 B。另外，数据分割处理 800 可以有利地通过产生附加的随机数在多个数据存储设施之间分配数据。数据可被分割为任意所希望的、所选择的、预定的或随机指定大小的单元，包括但不限于位，多个位，字节，千字节，兆字节或更大的，或大小的任意组合或序列。另外，分割处理中产生的不同大小的数据单元可以致使更难以将数据恢复为可用形式，从而增加了敏感数据的安全性。本领域的普通技术人员容易明了，分割数据单

元大小可以是各种数据单元大小或大小模式或大小组合。例如，数据单元大小可被选择为或预定为全部是相同大小、不同大小的固定集合，几种大小组合，或随机产生的大小。类似地，数据单元可根据固定或预定数据单元大小，数据单元大小的模式或组合，或随机产生的数据单元大小或每份的大小被分配到一个或多个份中。

[0134] 如前所述，为了重建敏感数据 S，数据部分需要被去随机化并且重新组装。这个处理可以有利地分别发生在验证引擎 215 和密码引擎 220 的数据组装模块 525 和 620 中。数字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，并且将数据重新组装为可用形式。例如，根据数据分割模块 520 采用图 8 的数据分割处理 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 中的至少两个数据存储设施的数据部分重建敏感数据 S。例如，这样分配 AC，AD，BC 和 BD 的配对，使得任意两个配对提供 A 和 B 或 C 和 D 之一。注意，S = A XOR B 或 S = C XOR D 指示当数据组装模块收到 A 和 B 或 C 和 D 之一时，数据组装模块 525 可以有利地重新组装敏感数据 S。因此，当例如其接收到来自数据存储设施 D1 到 D4 的至少头两个数据存储设备的数据部分时，数据组装模块 525 可以组装敏感数据 S，以响应授信引擎 110 的组装请求。

[0135] 基于上述数据分割和组装处理，敏感数据 S 仅在授信引擎 110 的有限区域内以可使用格式存在。例如，当敏感数据 S 包括登记验证数据时，仅在验证引擎 215 中可以获得可使用的未随机化的登记验证数据。类似地，当敏感数据 S 包括私有密码密钥数据时，仅在密码引擎 220 中可以获得可以使用的未随机化的私有密码密钥数据。

[0136] 虽然参考其优选实施例公开了数据分割和组装处理，本发明不旨在局限于此。而是本领域的技术人员将从此处的公开中认识到用于分割和重新组装敏感数据 S 的多种替代方案。例如，可以使用公钥加密进一步保护数据存储设施 D1 到 D4 处的数据。另外，本领域的普通技术人员容易明了，此处描述的数据分割模块也是本发明的单独的不同的实施例，其可结合到任意已有计算机系统、软件套件、数据库或其组合，或本发明的其他实施例，诸如此处公开和描述的授信引擎、验证引擎和事务处理引擎内，与其组合在一起、或成为其一部分。

[0137] 图 9A 示出了根据本发明的实施例的方面的登记处理 900 的数据流。如图 9A 所示，当用户希望在密码系统 100 的授信引擎 110 上登记时，登记处理 900 在步骤 905 开始。根据这个实施例，用户系统 105 有利地包括客户机侧小程序，诸如询问用户以便输入登记诸如人口统计学数据和登记验证数据的基于 Java 的小程序。根据一个实施例，登记验证数据包括用户 ID，口令（多个），生物测定（多个）等。根据一个实施例，在询问处理过程中，客户机侧小程序优选地与授信引擎 110 通信，以便确保选择的用户 ID 是唯一的。当用户 ID 不唯一时，授信引擎 110 可以有利地建议唯一的用户 ID。客户机侧小程序收集登记数据，并且例如通过 XML 文档将登记数据传输到授信引擎 110，并且特别地传输到事务处理引擎 205。根据一个实施例，以验证引擎 215 的公钥对传输编码。

[0138] 根据一个实施例，用户在登记处理 900 的步骤 905 过程中执行单个登记。例如，用户将他或她自己登记为特定人员，诸如 Joe user。当 Joe user 希望以 Joe user，Mega 公司的 CEO 登记时，那么根据这个实施例，Joe user 第二次登记，接收第二个唯一用户 ID，授信引擎 110 便不将两个身份相关联。根据本发明的另一个实施例，登记处理 900 为单个用户 ID 提供多个用户身份。因此，在上面的例子中，授信引擎 110 有利地将 Joe user 的两个身

份相关联。如本领域的技术人员将从此处的公开中理解的，用户可以具有许多身份，例如，Joe user 户主，Joe user 慈善基金会成员等。尽管用户可以具有多个身份，根据这个实施例，授信引擎 110 优选地仅存储一组登记数据。另外，当需要时用户可以有利地增加、编辑 / 更新或删除身份。

[0139] 虽然参考其优选实施例公开了登记处理 900，本发明不旨在局限于此。而是本领域的技术人员将从此处的公开中认识到用于收集登记数据并且特别是登记验证数据的多种替换方案。例如，小程序可以是基于公共对象模型 (COM) 的小程序等。

[0140] 在另一方面，登记处理可以包括分级登记。例如，最低级别的登记，用户可以在通信链路 125 上登记而不产生关于他或她的身份的文档。根据一种增加级别的登记，用户使用可信的第三方诸如数字公证人登记。例如用户可以亲自到可信的第三方，出示诸如出生证明、驾照、军人 ID 等的凭证，并且可信的第三方可以有利地在登记递交中包括例如其数字签名。可信的第三方可以包括实际公证人、诸如邮局或车辆管理局的政府机构、大公司中的登记雇员的人事人员等。本领域的技术人员将从此处的公开中理解，在登记处理 900 过程中可以发生多种不同级别的登记。

[0141] 在接收登记验证数据之后，在步骤 915，事务处理引擎 205 使用常规的全 SSL 技术将登记验证数据转发到验证引擎 215。在步骤 920，验证引擎 215 使用验证引擎 215 的私钥对登记验证数据解密。另外，验证引擎 215 采用数据分割模块对登记验证数据进行数学操作，以便将该数据分割为至少两个独立的不可译码的随机化的数字。如前所述，至少两个数字可以包括在统计上随机的数字和二进制异或的数字。在步骤 925，验证引擎 215 将随机化数字的每个部分转发到数据存储设施 D1 到 D4 之一。如前所述，验证引擎 215 还可以随机化将哪个部分传输到哪个仓库。

[0142] 通常在登记处理 900 过程中，用户还希望颁发数字证书，从而他或她可以从其他外部密码系统 100 接收加密文档。如前所述，证书颁发机构 115 一般地根据若干常规标准中的一个或多个颁发数字证书。一般地，数字证书包括每个人所知的用户或系统的公钥。

[0143] 不论用户是否在登记时或在另一个时刻请求数字证书，该请求通过授信引擎 110 被传输到验证引擎 215。根据一个实施例，请求包括具有例如用户的正确名称的 XML 文档。根据步骤 935，验证引擎 215 将该请求传输到密码引擎 220，指示密码引擎 220 产生密码密钥或密钥对。

[0144] 在请求之后，在步骤 935，密码引擎 220 产生至少一个密码密钥。根据一个实施例，密码处理模块 625 产生密钥对，其中一个密钥用作私钥，并且另一个用作公钥。密码引擎 220 存储私钥，并且根据一个实施例，存储公钥的拷贝。在步骤 945，密码引擎 220 将对数字证书的请求传输到事务处理引擎 205。根据一个实施例，该请求有利地包括标准化的请求，诸如嵌入在例如 XML 文档内的 PKCS10。对数字证书的请求可以有利地相应于一个或多个证书颁发机构和该证书颁发机构要求的一个或多个标准格式。

[0145] 在步骤 950，事务处理引擎 205 将这个请求转发到证书颁发机构 115，在步骤 955，证书颁发机构 115 返回数字证书。返回的数字证书可以有利地为诸如 PKCS7 的标准化格式，或一个或多个证书颁发机构 115 的专用格式。在步骤 960，由事务处理引擎 205 接收数字证书，并且将一个拷贝转发给用户，并且用授信引擎 110 存储一个拷贝。授信引擎 110 存储证书的一个拷贝，从而授信引擎 110 不需要依赖证书颁发机构 115 的可获得性。例如，当

用户希望发送数字证书或第三方请求用户的数字证书时，对数字证书的请求通常被发送到证书颁发机构 115。然而，如果证书颁发机构 115 正在进行维护，或已经出现故障或受到安全危及，可能不可获得数字证书。

[0146] 在颁发密码密钥之后的任意时刻，密码引擎 220 可以有利地采用上述的数据分割处理 800，从而将密码密钥分割为独立的不可译码的随机化的数字。类似于验证数据，在步骤 965，密码引擎 220 将随机化的数字传输到数据存储设施 D1 到 D4。

[0147] 本领域的技术人员将从此处的公开中认识到，用户可以在登记之后的任意时刻请求数字证书。另外系统间的通信可以有利地包括全 SSL 或公钥加密技术。另外，登记处理可以从多个证书颁发机构颁发多个数字证书，包括授信引擎 110 之内或之外的一个或多个私有证书颁发机构。

[0148] 如步骤 935 到 960 中公开的，本发明的一个实施例包括对最终存储在授信引擎 110 上的证书的请求。根据一个实施例，由于密码处理模块 625 颁发授信引擎 110 所使用的密钥，每个证书对应于一个私钥。因此，通过监视用户所拥有的或与用户相关联的证书，授信引擎 110 可以有利地提供互操作性。例如，当密码引擎 220 收到对密码功能的请求时，密码处理模块 625 可以审查进行请求的用户所拥有的证书，以便确定用户是否拥有与该请求的属性匹配的私钥。当这种证书存在时，密码处理模块 625 可以使用该证书或与其相关联的公钥或私钥执行所请求的功能。当这种证书不存在时，密码处理模块 625 可以有利地并且透明地执行若干活动，以便试图补救适当密钥的缺失。例如，图 9B 示出了互操作性处理 970 的流程图，其根据本发明的实施例的方面公开了确保密码处理模块 625 使用适当的密钥执行密码功能的上述步骤。

[0149] 如图 9B 所示，互操作性处理 970 以步骤 972 开始，其中密码处理模块 925 确定所希望的证书的类型。根据本发明的一个实施例，可以有利地在对密码功能的请求或由请求者提供的其他数据中指定证书类型。根据另一个实施例，可根据请求的格式确定证书类型。例如，密码处理模块 925 可以有利地识别相应于特定的类型的请求。

[0150] 根据一个实施例，证书类型可以包括一个或多个算法标准，例如，RSA，ELGAMAL 等。另外，证书类型可以包括一个或多个密钥类型，诸如对称密钥，公钥，诸如 256 位密钥的强加密密钥，弱安全密钥等。另外，证书类型可以包括升级或取代一个或多个上述算法标准或密钥、一个或多个消息或数据格式、诸如 Base32 或 Base64 的一个或多个数据封装或编码方案。证书类型还可以包括与一个或多个第三方密码应用或接口、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。本领域的技术人员将从此处的公开中认识到，证书类型中可以存在其他不同，并且可以如此处所公开的那样实现这些不同之间的来回转换。

[0151] 一旦密码处理模块 625 确定了证书类型，互操作性处理 970 进入步骤 974，并且确定用户是否拥有与步骤 974 中确定的类型相匹配的证书。当用户拥有匹配的证书，例如，授信引擎 110 可以例如通过其以前的存储器访问匹配的证书时，密码处理模块 825 知道匹配的私钥也被存储在授信引擎 110 内。例如，匹配的私钥可以存储在仓库 210 或仓库系统 700 内。密码处理模块 625 可以有利地请求从例如仓库 210 汇集匹配的私钥，然后在步骤 976，使用匹配的私钥执行密码活动或功能。例如，如前所述，密码处理模块 625 可以有利地执行散列，散列比较，数据加密或解密，数字签名检验或创建等。

[0152] 当用户不拥有匹配的证书时，互操作性处理 970 进入步骤 978，其中密码处理模块

625确定用户是否拥有交叉认证的证书。根据一个实施例，当第一证书颁发机构确定信任来自第二证书颁发机构的证书时，发生证书颁发机构之间的交叉认证。换言之，第一证书颁发机构确定来自第二证书颁发机构的证书满足某些质量标准，并且因此可被“证明”为等同于第一证书颁发机构自己的证书。当证书颁发机构颁发例如具有多个信任级别的证书时，交叉认证变得更为复杂。例如，第一证书颁发机构可能，通常基于登记处理的可靠性程度，为特定证书提供三种信任级别，而第二证书颁发机构可能提供七种信任级别。交叉认证可以有利地追踪可以用第二证书颁发机构的哪些级别和哪些证书取代第一证书颁发机构的哪些级别和哪些证书。当在两个证书颁发机构之间正式地公开地进行上述交叉认证时，证书和级别彼此之间的映射通常称为“链”。

[0153] 根据本发明的另一个实施例，密码处理模块625可以有利地开发证书颁发机构达成协议的那些交叉认证之外的交叉认证。例如，密码处理模块625可以访问第一证书颁发机构的证书操作声明(CPS)或其他发表的政策声明，并且使用例如特定信任级别所需的验证标记，将第一证书颁发机构的证书匹配到另一个证书颁发机构的那些证书。

[0154] 当在步骤978中密码处理模块625确定用户拥有交叉认证的证书时，互操作性处理970进入步骤976，并且使用交叉认证的公钥、私钥或这两者执行密码活动或功能。可替换地，当密码处理模块625确定用户不拥有交叉认证证书时，互操作性处理970进入步骤980，其中密码处理模块625选择颁发所请求的证书类型或交叉认证证书的证书颁发机构。在步骤982，密码处理模块625确定前面讨论的用户登记验证数据是否满足选择的证书颁发机构的验证要求。例如，如果用户在网络上通过例如回答人口统计和其他问题登记，所提供的验证数据可以建立比提供生物测定数据和亲临诸如例如公证人处的第三方的用户低的信任级别。根据一个实施例，可以有利地在选择的证书颁发机构的CPS中提供上述验证要求。

[0155] 当用户给授信引擎110提供了满足选择的证书颁发机构的要求的登记验证数据时，互操作性处理970进入步骤984，其中密码处理模块825从选择的证书颁发机构获取证书。根据一个实施例，密码处理模块625通过登记处理900的下列步骤945到960获取证书。例如，密码处理模块625可以有利地采用密码引擎220已经可用的一个或多个密钥对中的一个或多个公钥从证书颁发机构请求证书。根据另一个实施例，密码处理模块625可以有利地产生一个或多个新的密钥对，并且使用相应的公钥从证书颁发机构请求证书。

[0156] 根据另一个实施例，授信引擎110可以有利地包括能够颁发一种或多种证书类型的一个或多个证书颁发模块。根据这个实施例，证书颁发模块可以提供上述的证书。当密码处理模块625获取证书时，互操作性处理970进入步骤976，并且使用相应于获取的证书的公钥、私钥或这两者执行密码活动或功能。

[0157] 当用户在步骤982中未向授信引擎110提供满足所选择的证书颁发机构的要求的登记验证数据时，密码处理模块625在步骤986确定是否存在具有不同验证要求的其他证书颁发机构。例如，密码处理模块625可以寻找具有较低验证要求但是仍然颁发所选择的证书或交叉认证的证书颁发机构。

[0158] 当存在具有较低要求的上述证书颁发机构时，互操作性处理970进入步骤980，并且选择该证书颁发机构。可替换地，当不存在这种证书颁发机构时，在步骤988，授信引擎110可以从用户处请求附加的验证标记。例如，授信引擎110可以请求包括例如生物测定数

据的新的登记验证数据。另外，授信引擎 110 可以要求用户亲临可信的第三方并且提供适当的验证凭证，诸如例如，在公证人目前出示驾照，社会保险卡，银行卡，出生证明，军人 ID 等。当授信引擎 110 收到更新的验证数据时，互操作性处理 970 进入步骤 984，并且获取上述选择的证书。

[0159] 通过上述的互操作性处理 970，密码处理模块 625 有利地提供不同密码系统之间的无缝的透明的转换和变换。本领域的技术人员将从此处的公开中认识到上述可互操作的系统的多种优点和实现。例如，互操作性处理 970 的上述步骤 986 可以有利地包括在下面更详细讨论的信任仲裁的方面，其中证书颁发机构可以在特殊情况下接受较低级别的交叉认证。另外，互操作性处理 970 可以包括确保诸如利用证书撤销列表 (CRL) 的标准证书撤销的利用，在线证书状态协议 (OCSP) 等之间的互操作性。

[0160] 图 10 示出了根据本发明的实施例的方面的验证处理 1000 的数据流。根据一个实施例，验证处理 1000 包括从用户处收集当前验证数据，并且将其与用户的登记验证数据进行比较。例如，验证处理 1000 在步骤 1005 开始，其中用户希望与例如提供方执行事务处理。这种事务处理可以包括例如选择购买选择、请求访问提供方系统 120 的受限区域或设备等。在步骤 1010，提供方给用户提供事务处理 ID 和验证请求。事务处理 ID 可以有利地包括具有与 128 位随机值相成串连接的 32 位时间戳的 192 位值，或与 32 位提供方特定常量相成串连接的“现时 (nonce)”。这种事务处理 ID 唯一地标识事务处理，从而授信引擎 110 可以拒绝模仿的事务处理。

[0161] 验证请求可以有利地包括特定的事务处理需要的验证级别。例如，提供方可以指定待决事务处理所需的特定置信级别。如果不能以这个置信级别进行验证，如下面所述，在没有对用户的进一步验证以便提升置信级别，或提供方和服务器之间关于验证的改变的情况下，不发生该事务处理。下面将更完整地讨论这些问题。

[0162] 根据一个实施例，可以有利地由提供方侧小程序或其他软件程序产生事务处理 ID 和验证请求。另外，事务处理 ID 和验证数据的传输可以包括使用常规 SSL 技术，诸如例如，1/2 SSL 或换言之提供方侧验证的 SSL 加密的一个或多个 XML 文档。

[0163] 在用户系统 105 收到事务处理 ID 和验证请求之后，用户系统 105 从用户处收集当前验证数据，其中潜在地包括当前生物测定信息。用户系统 105 在步骤 1015 以验证引擎 215 的公钥至少对当前验证数据“B”和事务处理 ID 加密，并且将该数据传输到授信引擎 110。该传输优选地包括至少以常规的 1/2 SSL 技术加密的 XML 文档。在步骤 1020，事务处理引擎 205 接收该传输，优选地识别数据格式或 URL 或 URI 中的请求，并且将该传输转发到验证引擎 215。

[0164] 在步骤 1015 和 1020 中，提供方系统 120 在步骤 1025 使用优选的全 SSL 技术将事务处理 ID 和验证请求转发到授信引擎 110。这个通信还可以包括提供方 ID，虽然还可以通过事务处理 ID 的非随机部分传输提供方标识。在步骤 1030 和 1035，事务处理引擎 205 接收该通信，在审查跟踪中创建记录，并且产生对将被从数据存储设施 D1 到 D4 中汇集的用户登记验证数据的请求。在步骤 1040，仓库系统 700 将相应于用户的登记验证数据的部分传输到验证引擎 215。在步骤 1045，验证引擎 215 使用其私钥解密该传输，并且对登记验证数据和用户提供的当前验证数据进行比较。

[0165] 步骤 1045 的比较可以有利地应用前面提及的并且在下面更详细讨论的启发式上

下文敏感的验证。例如，如果接收的生物测定信息不能完美匹配，则产生较低的置信匹配。在特定实施例中，验证的置信级别和事务处理的属性以及用户与提供方这两者所希望的相平衡。同样这将在下面更详细地讨论。

[0166] 在步骤1050，验证引擎215以步骤1045的比较结果填充验证请求。根据本发明的一个实施例，以验证处理1000的YES/NO或TRUE/FALSE结果填充验证请求。在步骤1055，将填充的验证请求返回给提供方，以便提供方采取行动，例如允许用户完成发起验证请求的事务处理。根据一个实施例，向用户传递确认消息。

[0167] 基于上述，验证处理1000有利地保持敏感数据的安全性，并且产生配置为保持敏感数据的完整性的结果。例如，敏感数据仅被汇集在验证引擎215内。例如，登记验证数据不可译码，直到其被数据汇集模块汇集在验证引擎215中为止，并且当前验证数据不可译码，直到其被以常规SSL技术和验证引擎215的私钥展开为止。另外，传输到提供方的验证结果不包括敏感数据，并且用户可能甚至不知道他或她是否产生了有效验证数据。

[0168] 虽然参考其优选和可替换的实施例公开了验证处理1000，本发明不旨在局限于此。而是本领域的技术人员将从此处的公开中认识到验证处理1000的多种替换方案。例如，可以有利地以几乎任意请求应用程序取代提供方，甚至那些驻留在用户系统105内的请求应用程序。例如，客户机应用程序，诸如Microsoft Word可以在解锁文档之前使用应用程序接口(API)或密码API(CAPI)请求验证。可替换地，邮件服务器，网络，蜂窝电话，个人或移动计算设备，工作站等全都可以做出可由验证处理1000填写的验证请求。事实上，在提供上述可信的验证处理1000之后，进行请求的应用程序或设备可以提供对多种电子或计算机设备或系统的访问或使用。

[0169] 另外，在验证失败的情况下，验证处理1000可以采用多种替换过程。例如，验证失败可以保持相同的事务处理ID，并且请求用户重新输入他或她的当前验证数据。如前所述，使用相同的事务处理ID允许验证引擎215的比较器监视并且限制针对特定事务处理的验证尝试次数，从而创建更安全的密码系统100。

[0170] 另外，可以有利地采用验证处理1000开发极好的单次登录解决方案，诸如解锁敏感数据库。例如，成功或肯定的验证可以给通过验证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，用户的验证可以给用户提供对与多个在线提供方、局域网、各种个人计算设备、Internet服务提供商、拍卖提供商、投资经纪人等相关联的口令、登录、金融凭证等的访问。通过采用敏感数据库，由于不再需要通过关联记忆口令，用户可以选择真正大和随机的口令。而是验证处理1000提供对它们的访问。例如，用户可以选择长度大于20个数字的随机字母数字串，而不是与可记忆的数据、名称等相关联的某些内容。

[0171] 根据一个实施例，与给定用户相关联的敏感数据库可以有利地存储在仓库210的数据存储设施内，或被分割并且存储在仓库系统700内。根据这个实施例，在肯定的用户验证之后，授信引擎110诸如例如给适当的口令或给进行请求的应用程序提供所请求的敏感数据。根据另一个实施例，授信引擎110可以包括用于存储敏感数据库的单独系统。例如，授信引擎110可以包括实现数据库功能并且被形容为驻留在授信引擎110的前述前端安全系统“之后”的独立软件引擎。根据这个实施例，在软件引擎从授信引擎110收到指示肯定的用户验证的信号之后，软件引擎提供所请求的敏感数据。

[0172] 在另一个实施例中，可由第三方系统实现该数据库。类似于软件引擎实施例，在第三方系统从授信引擎 110 收到指示肯定的用户验证的信号之后，第三方系统可以有利地提供所请求的敏感数据。根据另一个实施例，可以在用户系统 105 上实现该数据库。在从授信引擎 110 收到指示肯定的用户验证的信号之后，用户侧软件引擎可以有利地提供前述的数据。

[0173] 虽然参考其可替换的实施例公开了前述的数据库，本领域的技术人员将从此处的公开中认识到其多种附加实现。例如，特定数据库可以包括前述实施例中的某些或全部方面。另外，任意前述数据库可以在不同时刻工作于一个或多个验证请求。例如，任意数据库可能需要以每一个或多个事务处理、周期地、每一个或多个会话、对一个或多个 Web 页面或 Web 站点的每次访问、以一个或多个其他的指定间隔等进行验证。

[0174] 图 11 示出了根据本发明的实施例的方面的签署处理 1100 的数据流。如图 11 所示，签署处理 1100 包括类似于前面参考图 10 描述的验证处理 1000 的那些步骤。根据本发明的一个实施例，签署处理 1100 首先验证用户，然后如下面更详细讨论的那样执行若干数字签名功能中的一个或多个。根据另一个实施例，签署处理 1100 可以有利地存储与其相关数据，诸如消息或文档的散列等。可以有利地在审查或任意其他情况中使用这种数据，诸如例如，当参与方试图抵赖事务处理时。

[0175] 如图 11 所示，在验证步骤中，用户和提供方可以有利地就消息诸如例如合同达成协议。在签署过程中，签署处理 1100 有利地确保用户签署的合同与提供方提供的合同一致。因此根据一个实施例，提供方和用户将其消息或合同的相应拷贝的散列包括在传输到验证引擎 215 的数据中。通过仅采用消息或合同的散列，授信引擎 110 可以有利地存储数目显著减少的数据，提供了更有效和更具成本效益的密码系统。另外，可以有利地对存储的散列和当前涉及的文档的散列进行比较，以便确定当前涉及的文档是否与由任意一方签署的文档匹配。确定文档是否与事务处理所涉及的文档一致的能力提供了可被用于对抗一方对事务处理的否认要求的附加证据。

[0176] 在步骤 1103，验证引擎 215 汇集登记验证数据，并且对其和用户提供的当前登记验证数据进行比较。当验证引擎 215 的比较器指出登记验证数据与当前验证数据匹配时，验证引擎 215 的比较器还对提供方提供的消息的散列和用户提供的消息的散列进行比较。因此，验证引擎 215 有利地确保用户同意的消息与提供方同意的消息一致。

[0177] 在步骤 1105，验证引擎 215 向密码引擎 220 传输数字签名请求。根据本发明的一个实施例，该请求包括消息或合同的散列。然而，本领域的技术人员将从此处的公开中认识到，密码引擎 220 可以对几乎任意类型的数据加密，包括但不限于，视频，音频，生物测定，图像或文本，以便形成所希望的数字签名。返回步骤 1105，数字签名请求优选地包括通过常规的 SSL 技术传递的 XML 文档。

[0178] 在步骤 1110，验证引擎 215 向数据存储设施 D1 到 D4 中的每一个传输请求，从而数据存储设施 D1 到 D4 中的每一个传输其相应于签署方的密码密钥或多个密钥的相应部分。根据另一个实施例，密码引擎 220 采用上面讨论的互操作性处理 970 的步骤中的某些或全部，从而密码引擎 220 首先确定为签署方从仓库 210 或仓库系统 700 请求的适当密钥或多个密钥，并且采取行动以便提供适当的匹配密钥。根据另一个实施例，验证引擎 215 或密码引擎 220 可以有利地请求与签署方相关联并且存储在仓库 210 或仓库系统 700 内的一个或

多个密钥。

[0179] 根据一个实施例，签署方包括用户和提供方之一或这两者。在这种情况下，验证引擎 215 有利地请求相应于用户和 / 或提供方的密码密钥。根据另一个实施例，签署方包括授信引擎 110。在这个实施例中，授信引擎 110 证明验证处理 1000 正确地验证了用户、提供方或这两者。因此，验证引擎 215 请求授信引擎 110 的密码密钥，诸如例如，属于密码引擎 220 的密钥，以便执行数字签名。根据另一个实施例，授信引擎 110 执行类似数字公证人的功能。在这个实施例中，签署方包括用户、提供方或这两者以及授信引擎 110。因此，授信引擎 110 提供用户和 / 或提供方的数字签名，然后以其自己的数字签名指出正确地验证了用户和 / 或提供方。在这个实施例中，验证引擎 215 可以有利地请求相应于用户，提供方或这两者的密码密钥的汇集。根据另一个实施例，验证引擎 215 可以有利地请求相应于授信引擎 110 的密码密钥的汇集。

[0180] 根据另一个实施例，授信引擎 110 执行委托类功能。例如，授信引擎 110 可以代表第三方数字地签署消息。在该情况下，验证引擎 215 请求与第三方相关联的密码密钥。根据这个实施例，签署处理 1100 可以有利地包括允许委托类功能之前的第三方验证。另外，验证处理 1000 可以包括对第三方限制的检查，诸如例如，规定何时并且在何种情况下可以使用特定第三方的签名的业务逻辑等。

[0181] 基于上文，在步骤 1110，验证引擎从数据存储设施 D1 到 D4 请求相应于签署方的密码密钥。在步骤 1115，数据存储设施 D1 到 D4 将其相应于签署方的密码密钥的相应部分传输到密码引擎 220。根据一个实施例，上文传输包括 SSL 技术。根据另一个实施例，可以有利地以密码引擎 220 的公钥对上面的传输进行超级加密。

[0182] 在步骤 1120，密码引擎 220 组装签署方的上述密码密钥并且以其对消息加密，从而形成数字签名（多个）。在签署处理 1100 的步骤 1125，密码引擎 220 将数字签名（多个）传输到验证引擎 215。在 1130，验证引擎 215 将填充的验证请求与散列消息的拷贝和数字签名（多个）一起传输到事务处理引擎 205。在步骤 1135，事务处理引擎 205 向提供方传输收据，包括事务处理 ID，对验证是否成功的指示，以及数字签名（多个）。根据一个实施例，上述传输可以有利地包括授信引擎 110 的数字签名。例如，授信引擎 110 可以采用其私钥对收据的散列加密，从而形成数字签名以便附加到对提供方的传输。

[0183] 根据一个实施例，事务处理引擎 205 还向用户传输确认消息。虽然参考其优选和替换实施例公开了签署处理 1100，本发明不旨在局限于此。而是本领域的技术人员将从此处的公开中认识到签署处理 1100 的多种替换方案。例如，可以用诸如电子邮件应用程序的用户应用程序取代提供方。例如，用户可能希望以他或她的数字签名数字地签署特定电子邮件。在这种实施例中，签署处理 1100 中的传输可以有利地仅包括消息的散列的一个拷贝。另外，本领域的技术人员将从此处的公开中认识到多种客户机应用程序可以请求数字签名。例如，客户机应用程序可以包括字处理器，电子表格，电子邮件，语音邮件，对受限系统区域的访问等。

[0184] 另外，本领域的技术人员将从此处的公开中认识到，签署处理 1100 的步骤 1105 到 1120 可以有利地采用图 9B 的互操作性处理 970 的步骤中的某些或全部，从而提供可能需要在不同签名类型下处理数字签名的不同密码系统之间的互操作性。

[0185] 图 12 示出了根据本发明的实施例的方面的加密 / 解密处理 1200 的数据流。如图

12 所示，解密处理 1200 通过使用验证处理 1000 验证用户而开始。根据一个实施例，验证处理 1000 在验证请求中包括同步会话密钥。例如，本领域的技术人员理解，在常规的 PKI 技术中，使用公钥和私钥加密或解密数据是数学密集的，并且可能需要大量系统资源。然而，在对称密钥密码系统中，或在消息的发送方和接收方共享用于加密和解密消息的单个公共密钥的系统中，数学操作显著地较为简单并且较快。因此，在常规的 PKI 技术中，消息的发送方将产生同步会话密钥，并且使用较简单、较快的对称密钥系统对消息加密。然后，发送方以接收方的公钥对会话密钥加密。加密的会话密钥将被附加到同步加密的消息上，并且这两种数据都被发送到接收方。接收方使用他或她的私钥对会话密钥解密，然后使用会话密钥解密该消息。基于上文，将较简单并且较快的对称密钥系统用于大部分加密 / 解密处理。因此，在解密处理 1200 中，解密有利地假设已经以用户的公钥对同步密钥进行了加密。因此如前所述，加密的会话密钥被包括在验证请求中。

[0186] 返回到解密处理 1200，在用户在步骤 1205 已被验证之后，验证引擎 215 将加密的会话密钥转发到密码引擎 220。在步骤 1210，验证引擎 215 向数据存储设施 D1 到 D4 中的每一个转发请求，请求用户的密码密钥数据。在步骤 1215，每个数据存储设施 D1 到 D4 将其密码密钥的相应部分传输到密码引擎 220。根据一个实施例，以密码引擎 220 的公钥对上述传输加密。

[0187] 在解密处理 1200 的步骤 1220，密码引擎 220 汇集密码密钥并且以其解密会话密钥。在步骤 1225，密码引擎将会话密钥转发到验证引擎 215。在步骤 1227，验证引擎 215 填充包括解密的会话密钥的验证请求，并且将填充的验证请求传输到事务处理引擎 205。在步骤 1230，事务处理引擎 205 将验证请求与会话密钥一起转发到进行请求的应用程序或提供方。然后根据一个实施例，进行请求的应用程序或提供方使用会话密钥对加密的消息进行解密。

[0188] 虽然参考其优选的和可替换的实施例公开了解密处理 1200，本领域的技术人员将从此处的公开中认识到解密处理 1200 的多种替换方案。例如，解密处理 1200 可以放弃同步密钥加密，并且依赖全公钥技术。在这种实施例中，进行请求的应用程序可将整个消息传输到密码引擎 220，或可以采用某种类型的压缩或可逆散列，以便将消息传输到密码引擎 220。本领域的技术人员将从此处的公开中认识到上述通信可以有利地包括以 SSL 技术打包的 XML 文档。

[0189] 加密 / 解密处理 1200 还提供了对文档或其他数据的加密。因此在步骤 1235，进行请求的应用程序或提供方可以有利地向授信引擎 110 的事务处理引擎 205 传输对用户的公钥的请求。由于进行请求的应用程序或提供方使用用户的公钥例如加密将被用于加密文档或消息的会话密钥，进行请求的应用程序或提供方做出这种请求。如在登记处理 900 中所述，事务处理引擎 205 例如在海量存储器 225 中存储用户的数字证书的拷贝。因此，在加密处理 1200 的步骤 1240，事务处理引擎 205 从海量存储器 225 请求用户的数字证书。在步骤 1245，海量存储 225 将相应于用户的数字证书传输到事务处理引擎 205。在步骤 1250，事务处理引擎 205 将该数字证书传输到进行请求的应用程序或提供方。根据一个实施例，加密处理 1200 的加密部分不包括用户的验证。这是由于进行请求的提供方仅需要用户的公钥，并且不需要任何敏感数据。

[0190] 本领域的技术人员将从此处的公开中认识到，如果特定用户不具有数字证书，授

信引擎 110 可以采用登记处理 900 中的某些或全部，以便为该特定用户产生数字证书。然后授信引擎 110 可以启动加密 / 解密处理 1200，并且因此提供适当的数字证书。另外，本领域的技术人员将从此处的公开中认识到，加密 / 解密处理 1200 的步骤 1220 和 1235 到 1250 可以有利地采用图 9B 的互操作性处理的步骤中的某些或全部，从而提供可能例如需要处理加密的不同密码系统之间的互操作性。

[0191] 图 13 示出了根据本发明的另一个实施例的几方面的授信引擎系统 1300 的简化方框图。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。为了便于更完整地理解本发明，图 13 将每个授信引擎 1305，1310，1315 和 1320 示出为具有事务处理引擎、仓库和验证引擎。然而，本领域的技术人员将认识到，每个事务处理引擎可以有利地包括参考图 1 到 8 公开的元件和通信通道中的某些、一种组合或其全部。例如，一个实施例可以有利地包括具有一个或多个事务处理引擎，仓库和密码服务器或其任意组合的授信引擎。

[0192] 根据本发明的一个实施例，授信引擎 1305，1310，1315 和 1320 中的每一个在地理上分离，从而例如授信引擎 1305 可以驻留在第一位置，授信引擎 1310 可以驻留在第二位置，授信引擎 1315 可以驻留在第三位置，并且授信引擎 1320 可以驻留在第四位置。上述的地理分离有利地减少了系统响应时间，同时提高了整个授信引擎系统 1300 的安全性。

[0193] 例如，当用户登录到密码系统 100 上时，用户可以距第一位置最近，并且可能希望被验证。如参考图 10 所述，为了进行验证，用户提供当前验证数据诸如生物测定等，并且对当前验证数据和用户的登记验证数据进行比较。因此，根据一个例子，用户有利地将当前验证数据提供给在地理上最近的授信引擎 1305。授信引擎 1305 的事务处理引擎 1321 然后将当前验证数据转发到同样驻留在第一位置的验证引擎 1322。根据另一个实施例，事务处理引擎 1321 将当前验证数据转发到授信引擎 1310，1315 或 1320 的验证引擎中的一个或多个。

[0194] 事务处理引擎 1321 还从例如授信引擎 1305 到 1320 中的每一个的仓库请求登记验证数据的汇集。根据这个实施例，每个仓库将其登记验证数据的部分提供给授信引擎 1305 的验证引擎 1322。然后验证引擎 1322 采用例如来自头两个仓库的加密数据部分做出响应，并且将登记验证数据组装为译码形式。验证引擎 1322 对登记验证数据和当前验证数据进行比较，并且将验证结果返回授信引擎 1305 的事务处理引擎 1321。

[0195] 基于上文，授信引擎系统 1300 采用多个在地理上分离的授信引擎 1305 到 1320 中最近的一个执行验证处理。根据本发明的一个实施例，可以有利地由在用户系统 105、提供方系统 120 或证书颁发机构 115 中的一个或多个上执行的客户机侧小程序处执行将信息路由到最近的事务处理引擎。根据可替换的实施例，可以采用更复杂的判定处理从授信引擎 1305 到 1320 中进行选择。例如，判定可以基于给定授信引擎的可获得性、可操作性、连接速度、负载、性能、地理接近程度或其组合。

[0196] 以这种方式，授信引擎系统 1300 降低了其响应时间，同时保持与地理上位于远方的数据存储设施相关联的安全性优点，诸如参考图 7 讨论的那些数据存储设施，其中每个数据存储设施存储敏感数据的随机化的部分。例如，危及授信引擎 1315 的仓库 1325 不必然危及授信引擎系统 1300 的敏感数据。这是由于仓库 1325 仅包含毫无用处的不可译码的随机化的数据，而没有更多部分。

[0197] 根据另一个实施例，授信引擎系统 1300 可以有利地包括被安排为类似于验证引擎的多个密码引擎。密码引擎可以有利地执行密码功能，诸如参考图 1-8 公开的那些密码功能。根据另一个实施例，授信引擎系统 1300 可以有利地以多个密码引擎取代多个验证引擎，从而执行诸如参考图 1-8 公开的那些密码功能。根据本发明的另一个实施例，如前面公开的，授信引擎系统 1300 可以用具有验证引擎、密码引擎或这两者的功能中的某些或全部的引擎取代多个验证引擎中的每一个。

[0198] 虽然参考其优选的和可替换的实施例公开了授信引擎系统 1300，本领域的技术人员将认识到授信引擎系统 1300 可以包括授信引擎 1305 到 1320 中的多个部分。例如，授信引擎系统 1300 可以包括一个或多个事务处理引擎，一个或多个仓库，一个或多个验证引擎，或一个或多个密码引擎或其组合。

[0199] 图 14 示出了根据本发明的另一个实施例的方面的授信引擎系统 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。根据一个实施例，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 的元件中的某些或全部。根据这个实施例，当用户系统 105，提供方系统 120，或证书颁发机构 115 的客户机侧小程序与授信引擎系统 1400 通信时，那些通信被发送到每个授信引擎 1405 到 1420 的 IP 地址。另外，每个授信引擎 1405，1410，1415 和 1420 的每个事务处理引擎类似于参考图 13 公开的授信引擎 1305 的事务处理引擎 1321 运行。例如，在验证处理过程中，每个授信引擎 1405，1410，1415 和 1420 的每个事务处理引擎将当前验证数据传输到其相应的验证引擎，并且传输请求以便组装存储在每个授信引擎 1405 到 1420 的每个仓库内的随机化数据。图 14 未示出全部这些通信；这样将使得图示过度复杂。继续验证处理，每个仓库然后将其随机化数据部分传输到每个授信引擎 1405 到 1420 的每个验证引擎。每个授信引擎的每个验证引擎采用其比较器确定当前验证数据是否与由每个授信引擎 1405 到 1420 的仓库提供的登记验证数据相匹配。根据这个实施例，每个验证引擎的比较结果然后被传输到另外三个授信引擎的冗余模块。例如，授信引擎 1405 的验证引擎的结果被传输到授信引擎 1410，1415 和 1420 的冗余模块。因此，授信引擎 1405 的冗余模块同样会收到授信引擎 1410，1415 和 1420 的验证引擎的结果。

[0200] 图 15 示出了图 14 的冗余模块的方框图。冗余模块包括配置为从三个验证引擎接收验证结果，并且将该结果传输到第四个授信引擎的事务处理引擎的比较器。该比较器对来自三个验证引擎的验证结果进行比较，并且如果这些结果中的两个一致，比较器得出验证结果应与这两个一致的验证引擎的结果相匹配的结论。然后将这个结果传输回相应于不与这三个验证引擎相关联的授信引擎的事务处理引擎。

[0201] 基于上文，冗余模块根据从这样的验证引擎接收的数据确定验证结果，这些验证引擎优选地在地理上远离冗余模块的授信引擎。通过提供这种冗余功能，授信引擎系统 1400 确保对授信引擎 1405 到 1420 之一的验证引擎的危及不足以危及该特定授信引擎的冗余模块的验证结果。本领域的技术人员将认识到，授信引擎系统 1400 的冗余模块功能还可被应用于每个授信引擎 1405 到 1420 的密码引擎。然而，图 14 未示出这种密码引擎通信以避免复杂化。另外，本领域的技术人员将认识到用于图 15 的比较器的多种可替换的验证结果冲突解决算法适用于本发明。

[0202] 根据本发明的另一个实施例，授信引擎系统 1400 可以有利地在密码比较步骤中

采用冗余模块。例如，在一方或多方在特定事务处理过程中提供的文档的散列比较中，可以有利地实现参考图 14 和 15 公开的前述冗余模块中的某些或全部。

[0203] 虽然根据某些优选的和可替换的实施例描述了上述发明，本领域的普通技术人员将从此处的公开中明了其他实施例。例如，授信引擎 110 可以颁发短期证书，其中私有密码密钥在预定的时间段中被发放给用户。例如，当前证书标准包括可被设置为在预定量的时间之后到期的有效字段。因此，授信引擎 110 可以向用户发放在例如 24 小时内有效的私钥。根据这种实施例，授信引擎 110 可以有利地颁发将与特定用户相关联的新的密码密钥对，然后发放新密码密钥对的私钥。然后，一旦发放了私有密码密钥，授信引擎 110 立刻终止这种私钥的任意内部有效使用，这是由于授信引擎 110 不再能够保证它的安全。

[0204] 另外，本领域的技术人员将认识到密码系统 100 或授信引擎 110 可以包括识别任意类型的设备的能力，诸如但不限于，膝上计算机，蜂窝电话，网络，生物测定设备等。根据一个实施例，这种识别可以来自在对特定服务的请求中提供的数据，诸如导致访问或使用的对验证的请求，对密码功能的请求等。根据一个实施例，上述请求可以包括唯一设备标识符，诸如例如，处理器 ID。可替换地，请求可以包括特定的可识别的数据格式中的数据。例如，移动和卫星电话通常不包括用于完整 X509.V3 强加密证书的处理能力，并且因此不能请求它们。根据这个实施例，授信引擎 110 可以识别出现的数据格式类型，并且仅以同样的方法响应。

[0205] 在上述系统的附加方面中，可以使用如下所述的各种技术提供上下文敏感的验证。上下文敏感的验证，例如图 16 所示，提供了不仅评估用户试图验证自身时所发送的实际数据，还评估关于该数据的产生和传递的环境的可能。如下所述，这种技术还可以支持用户和授信引擎 110 之间或提供方和授信引擎 110 之间特定于事务处理的信任仲裁。

[0206] 如上所述，验证是证明用户是其所声称的人的处理。一般地，验证需要向验证机构证明某些事实。本发明的授信引擎 110 代表用户必须向其验证自身的机构。用户必须通过下面方法中的任意一种向授信引擎 110 证明他是其所声称的人：知道某些仅有该用户才应当知道的内容（基于知识的验证），具有某些仅有该用户才应当具有的内容（基于标记的验证），或是处于某些仅有该用户才应当如此的状态（基于生物测定的验证）。

[0207] 基于知识的验证的例子包括但不限于口令，PIN 号，或锁组合。基于标记的验证的例子包括但不限于房屋钥匙，物理信用卡，驾照，或特定电话号码。基于生物测定的验证的例子包括但不限于指纹，笔迹分析，面部扫描，手扫描，耳扫描，虹膜扫描，血管模式，DNA，声音分析，或视网膜扫描。

[0208] 每种验证类型具有特定的优点和缺点，并且每一种提供了不同级别的安全性。例如，与偷听别人的口令并且重复它相比，一般更难以创建与别人匹配的伪造的指纹。每种验证还需要验证机构知道不同类型的数据，以便使用该形式的验证检验某人。

[0209] 如此处使用的，“验证”广泛地指检验某人的身份是其所声称的全部处理。“验证”技术指基于特定知识、物理标记或生物测定读数的特定类型的验证。“验证数据”指向验证机构发送或证明以便确定身份的信息。“登记数据”指最初提交给验证机构以便建立用于与验证数据进行比较的基线的数据。“验证实例”指与以一种验证技术进行验证的尝试相关联的数据。

[0210] 参考上面的图 10 描述了验证用户的处理中所涉及的内部协议和通信。这个处理

中的发生上下文敏感验证的部分出现在作为图 10 的步骤 1045 示出的比较步骤中。这个步骤发生在验证引擎 215 内，并且涉及组装从仓库 210 取回的登记数据 410，并且将用户提供的验证数据与其进行比较。在图 16 示出并且在下面描述了这个处理的一个特定实施例。

[0211] 在图 16 的步骤 1600 由验证引擎 215 接收用户提供的当前验证数据和从仓库 210 取回的登记数据。这两组数据都可以包含与各个验证技术相关的数据。验证引擎 215 可以在步骤 1605 分离与每个单独验证实例相关联的验证数据。这是对验证数据和用户的登记数据的适当子集进行比较所必须的（例如，指纹验证数据应当与指纹登记数据而不是口令登记数据比较）。

[0212] 一般地，取决于哪些验证技术对于用户来说可用，对用户进行验证涉及一个或多个验证实例。这些方法受用户在其登记处理过程中提供的登记数据（如果用户在登记时未提供视网膜扫描，他不能使用视网膜扫描验证自己），以及用户当前可以使用的装置（例如，如果用户在其当前位置不具有指纹读取器，指纹验证是不现实的）的限制。在某些情况下，单个验证实例可能足以验证用户；然而，在某些情况下，可以使用多个验证实例的组合，以便为特定事务处理更确信地验证用户。

[0213] 每个验证实例由与特定验证技术（例如，指纹，口令，智能卡等）和为该特定技术捕捉和传递数据的环境有关的数据组成。例如，试图通过口令验证的特定实例不仅将产生与口令自身有关的数据，而且还产生与口令尝试相关的被称为“元数据”的环境数据。这种环境数据包括诸如下面的信息：特定验证实例发生的时间，传递验证信息的网络地址，以及可以确定的关于验证数据的起源的本领域技术人员知道的任意其他信息（连接类型，处理器序列号等）。

[0214] 在许多情况下，仅可获得少量的环境元数据。例如，如果用户位于使用代理或网络地址变换或掩盖原始计算机地址的其他技术的网络上，仅可以确定代理或路由器的地址。类似地，在许多情况下，由于禁止了系统操作员的这种特征的硬件或所使用的操作系统的限制，或用户系统和授信引擎 110 之间的连接的其他限制，不能获得诸如处理器序列号的信息。

[0215] 如图 16 所示，一旦在步骤 1605 提取和分离了验证数据中出现的各种验证实例，验证引擎 215 评估每个实例指示用户是其所声称的人的可靠性。一般基于若干因素确定单个验证实例的可靠性。这些可被分组为在步骤 1610 评估的与验证技术相关联的关于可靠性的因素，和在步骤 1815 评估的与提供的特定验证数据的可靠性有关的因素。第一组包括但不限于使用的验证技术的固有可靠性，和该方法使用的登记数据的可靠性。第二组包括但不限于登记数据与验证实例提供的数据之间的匹配程度，以及与验证实例相关联的元数据。这些因素中的每一个可被独立于其他因素改变。

[0216] 验证技术的固有可靠性基于冒充者提供别人的正确数据的困难程度，以及验证技术的整体错误率。对于基于口令和知识的验证方法，由于不能防止某人向另一人透露其口令并且第二个人使用该口令，这种可靠性通常相当低。由于知识可被相当容易地从一个人传递到另一个人，即使更复杂的基于知识的系统也可能仅具有中等的可靠性。由于不能保证正确的人持有正确的标记，基于标记的验证，诸如采用正确的智能卡或使用特定终端执行验证，与其自身使用具有类似的低可靠性。

[0217] 然而，生物测定技术固有地更为可靠，这是由于即使是有意地，一般难以用常规方

式给别人提供使用你自己的指纹的能力。由于破坏生物测定验证技术更为困难，生物测定方法的固有可靠性一般高于纯粹的基于知识或标记的验证技术。然而，即使是生物测定技术也可能具有产生伪接受或伪拒绝的某些情况。可以通过相同生物测定技术的不同实现的不同可靠性反映出这些情况。例如，由于使用更高质量的光学器件，或更好的扫描分辨率，或减少误接受或误拒绝发生的某些其他改进，由一个公司提供的指纹匹配系统可能提供比一个不同公司所提供的更高的可靠性。

[0218] 注意可以用不同方式表达这种可靠性。希望以可由启发 530 和验证引擎 215 的算法使用以便计算每个验证的置信级别的某个度量表达可靠性。表达这些可靠性的一种优选模式是表达为百分比或分数。例如，可将固有可靠性 97％分配给指纹，而可以仅将 50％的固有可靠性分配给口令。本领域的技术人员将认识到这些特定的值仅是示例性的，并且可以在不同实现方式之间改变。

[0219] 必须评定可靠性的第二个因素是登记的可靠性。这是上述“分级登记”处理的一部分。这个可靠性因素反映了在初始登记处理过程中提供的标识的可靠性。例如，如果个人最初以向公证人或其他公共官员物理地出示其身份证明的方式登记，并且在该时刻记录登记数据并且进行了公证，该数据比在登记过程中在网络上提供的并且仅以未真正绑定到该个人的数字签名或其他信息保证的数据更可靠。

[0220] 具有不同可靠性级别的其他登记技术包括但不限于：在授信引擎 110 操作员的物理部门登记；在用户的工作位置登记；在邮局或交通部门登记；通过授信引擎 110 操作员的分支方或可信方登记；匿名或冒名登记，其中登记的身份与特定真实个体不一致，以及本领域已知的这种其他方式。

[0221] 这些因素反映授信引擎 110 和在登记处理过程中提供的标识的来源之间的信任度。例如，如果在提供身份证据的初始处理过程中与雇员相关联地执行登记，对于公司内部来说，该信息可被认为极其可靠，但是被政府机构或竞争者信任的程度可能较低。因此，由这些其他组织操作的授信引擎可给该登记分配不同级别的可靠性。

[0222] 类似地，在网络上提交的但被以在相同授信引擎 110 的以前登记过程中提供的其他可信数据验证的附加数据可被如同原始登记数据认为是可靠的，即使该稍后数据是在开放网络上提交的。在这种情况下，随后的公证将有效地提高与原始登记数据相关联的可靠性级别。以这种方法为例，通过向某个登记官员证明与登记数据匹配的个体身份，则匿名或冒名登记可被提升为完全登记。

[0223] 上述可靠性因素一般为可以在任意特定验证实例之前确定的值。这是由于它们基于登记和技术而不是实际验证。在一个实施例中，基于这些因素产生可靠性的步骤涉及寻找针对该特定验证技术的以前确定的值和用户的登记数据。在本发明的有利实施例的另一个方面，这种可靠性可被包括在登记数据自身中。以这种方式，这些因素可被与从仓库 210 发送的登记数据一起自动地传递给验证引擎 215。

[0224] 虽然一般在任意单个验证实例之前确定这些因素，它们仍然对为用户使用特定验证技术的每个验证实例具有影响。另外，虽然值可能随着时间而改变（例如，如果用户以更可靠的方式重新登记），它们不依赖于验证数据本身。相反，与单个特定实例的数据相关联的可靠性因素可以在每个场合改变。如下所述必须为每个新验证评估这些因素，以便在步骤 1815 产生可靠性评分。

[0225] 验证数据的可靠性反映用户在特定验证实例中提供的数据和在验证登记过程中提供的数据之间的匹配。这是验证数据是否与用户所声称的个体的登记数据匹配的基本问题。通常当数据不匹配时，认为用户未被成功地验证并且验证失败。对其进行评估的方式可以根据使用的验证技术而改变。由如图 5 所示的验证引擎 215 的比较器 515 功能执行这种数据的比较。

[0226] 例如，一般以二值方式评估口令的匹配。换言之，口令或是完美匹配或是失配。通常不希望接受如果不是完全正确，接近正确口令的部分匹配口令。因此当评估口令验证时，比较器 515 返回的验证可靠性通常为 100％（正确）或 0％（错误），不可能为中间值。

[0227] 与口令类似的规则一般适用于基于标记的验证方法，诸如智能卡。这是由于具有带有类似标识符的智能卡或与正确的相类似的智能卡仍然和具有任意其他不正确的标记一样错误。因此标记也趋于二值验证：用户或是具有正确的标记或者没有。

[0228] 然而，某些类型的验证数据诸如调查表和生物测定一般不是二值验证。例如，指纹可能不同程度地与参考指纹匹配。在某种程度上，这可能是由于在初始登记或在后续验证过程中捕捉的数据的质量的改变。（指纹可能被弄脏或一个人可能具有愈合中的伤痕或灼伤了特定手指）。在其他情况下，由于信息自身可变的并且基于模式识别，数据可能不是完美匹配。（由于背景噪声或录制语音的环境声音，或由于这个人感冒了，语音分析可能感觉接近但不是完全正确）。最后，在比较大量数据的情况下，情况可能是大部分数据很好地匹配但是某些不是。(10 个问题的调查表可能产生关于个人问题的 8 个正确回答，和 2 个不正确回答）。出于这些原因中的任意原因，可能希望由比较器 515 给登记数据和用于特定验证实例的数据之间的匹配分配一个部分匹配值。以这种方式，例如可以说指纹 85％匹配，声纹 65％匹配，并且调查表 80％匹配。

[0229] 比较器 515 产生的这种测量（匹配程度）是表示验证是否正确的基本问题的因素。然而如上所述，这仅是可用于确定给定验证实例的可靠性的因素之一。还应注意即使可以确定某个部分程度的匹配，最终可能希望提供基于部分匹配的二值结果。在另一种操作模式中，还可以基于匹配程度是否超出特定的匹配阈值级别，将部分匹配视为是二值的，即，或是完美的 (100％）或是失败的 (0％）匹配。这种处理可用于为产生部分匹配的系统提供单一的匹配通过 / 失败级别。

[0230] 评估给定验证实例的可靠性所考虑的另一个因素与提供这个特定实例的验证数据的环境有关。如上所述，该环境指与特定验证实例相关联的元数据。这可以包括但不限于这样的信息，诸如：验证人的网络地址，就其可被确定而言；验证的时间；验证数据的传输模式（电话线，蜂窝电话，网络等）；和验证人的系统的序列号。

[0231] 这些因素可被用于产生用户通常请求的验证类型的简档。然后这种信息可被用于以至少两个方式评价可靠性。一种方式是用户是否以与这个用户的通常验证简档相一致的方式请求验证。如果用户通常在上班时间（当她在工作时）从一个网络地址，并且在晚上或周末（当她在家时）从一个不同的网络地址做出验证请求，由于在通常的验证简档之外，在上班时间从家庭地址发生的验证不太可靠。类似地，如果用户通常在晚上使用指纹生物测定验证，在白天仅使用口令发生的验证不太可靠。

[0232] 可以使用环境元数据评估验证实例的可靠性的一种附加方式是确定该环境提供关于验证人是其所声称的个体的确证程度。例如，如果验证来自具有已知与用户相关联的

序列号的系统，这是用户是其所声称的人的良好的环境指示器。相反，当已知用户居住在伦敦时，如果验证来自已知位于洛杉矶的网络地址，基于其环境这指示这个验证不太可靠。

[0233] 还可以在用户与提供方系统或与授信引擎 110 交互时使用的系统上放置 cookie 或其他电子数据。这些数据被写到用户的系统的存储设备内，并且可以包含可由 Web 浏览器或用户系统上的其他软件读取的标识。如果允许该数据在会话之间驻留在用户系统上（“永久 cookie”），其可被作为在特定用户的验证过程中对这个系统的过去使用的进一步证据的验证数据一起发送。事实上，给定实例的元数据，特别是永久 cookie 自身可以形成一种基于标记的验证器。

[0234] 一旦如上面在步骤 1610 和 1615 中分别所述产生了基于技术和验证实例数据的适当可靠性因子，它们可被用于在步骤 1620 产生验证实例的整体可靠性。一种这样作的方式是简单地将每个可靠性表达为百分数，并且将它们相乘在一起。

[0235] 例如，假设验证数据被完全根据用户过去的验证简档从已知是用户的家庭计算机的网络地址发送（100％），并且使用的技术是指纹识别（97％），并且通过用户的雇主向授信引擎 110 注册最初的指纹数据（90％），并且验证数据和登记数据中的原始指纹模板之间的匹配非常好（99％）。这个验证实例的整体可靠性被计算为这些可靠性的积：可靠性 100％ ×97％ ×90％ ×99％ -86.4％。

[0236] 这个计算的可靠性表示单个验证实例的可靠性。还可以使用不同地对待不同的可靠性因子的技术计算单个验证实例的整体可靠性，例如通过使用给每个可靠性因子分配不同权重的公式。另外，本领域的技术人员将认识到使用的实际值可以表示百分数之外的值，并且可以使用非算术系统。一个实施例可以包括验证请求人用于设置每个因子的权重和建立验证实例的整体可靠性时使用的算法的模块。

[0237] 如步骤 1620 指示的，验证引擎 215 可以使用上述技术和其变体确定单个验证实例的可靠性。然而，其可用于同时提供多个验证实例的许多验证情况。例如，当试图使用本发明的系统验证自身时，用户可以提供用户标识，指纹验证数据，智能卡和口令。在该情况下，三个独立的验证实例被提供给授信引擎 110 进行评估。如果验证引擎 215 确定由用户提供的数据包括多于一个验证实例，则进入步骤 1625，然后如步骤 1630 所示依次选择每个实例，并且如上面步骤 1610，1615 和 1620 中所述对其进行评估。

[0238] 注意所讨论的许多可靠性因子可以随着这些实例而改变。例如，这些技术的固有可靠性以及验证数据和登记数据之间提供的匹配程度很可能不同。另外，用户可能在不同时间在不同环境下为这些技术中的每一个提供登记数据，这也为这些实例中的每一个提供了不同的登记可靠性。最后，即使为这些实例中的每一个提交数据的环境相同，对这些技术的使用可能各自不同适合于用户简档，并且从而可被分配不同的环境可靠性（例如，用户可能通常使用其口令和指纹而不是其智能卡）。

[0239] 结果，这些验证实例中的每一个的最终可靠性可能彼此不同。然而，通过一起使用多个实例，验证的整体置信级别趋于增加。

[0240] 一旦验证引擎为在验证数据中提供的所有验证实例执行了步骤 1610 到 1620，在步骤 1635 使用每个实例的可靠性评估整体验证置信级别。可用关于产生的各个可靠性的各种方法为将各个验证实例可靠性组合为验证置信级别的这个处理建模，并且还可能解决这些验证技术中的某些之间的特定交互（例如，多个基于知识诸如口令的系统可能产生低

于单个口令，并且甚至低于相当弱的生物测定，诸如基本语音分析的置信）。

[0241] 验证引擎 215 组合多个并发验证实例的可靠性，以便产生最终置信级别的一种方法是对每个实例的不可靠性相乘以便获得总的不可靠性。该不可靠性一般是可靠性的互补百分比。例如，84％可靠的技术的不可靠性为 16％。产生可靠性 86％，75％和 72％的上述 3 个验证实例（指纹，智能卡，口令）分别具有相应的不可靠性 (100-86)％，(100-75)％和 (100-72)％，或 14％，25％和 28％。通过对这些不可靠性相乘，得到累积不可靠性 14％ ×25％ ×28％ -.98％，这相应于 99.02％的可靠性。

[0242] 在一种附加的操作模式中，可以在验证引擎 215 中应用附加的因子和启发 530，以便说明各种验证技术的互相依赖。例如，如果某人未被授权访问特定的家用计算机，他们可能也不能使用相同地址的电话线。因此，基于发起电话号码以及验证系统的序列号的验证不会对验证的整体置信带来很大增加。然而，基于知识的验证极大地独立于基于标记的验证（即，如果某人偷了你的蜂窝电话或钥匙，他们不太可能知道你的 PIN 或口令）。

[0243] 另外，不同的提供方或其他验证请求人可能希望不同地加权验证的不同方面。这可以包括使用单独的加权因子或用于计算各个实例的可靠性的算法，以及使用不同的方法评估具有多个实例的验证事件。

[0244] 例如，某些类型的事务处理例如公司的电子邮件系统的提供方可能希望默认地主要基于启发和其他环境数据进行验证。因此，他们给关于元数据相关的因子和与围绕验证事件的环境相关联的信息有关的其他简档应用高权重。由于仅需要用户在上班时间登录到正确的机器，这种安排可用于减轻用户在通常操作时间中的负担。然而，由于一种技术最适合于出于特定提供方目的的验证的决策，其他提供方可能最重地给来自特定技术的验证加权，例如指纹匹配。

[0245] 在一种操作模式中，可由验证请求人在产生验证请求时定义这种改变的权重，并且将其与验证请求一起发送到授信引擎 110。在另一种操作模式中，还可以在验证请求人的初始登记处理过程中将这些操作设置为偏好，并且存储在验证引擎内。

[0246] 一旦验证引擎 215 为提供的验证数据产生了验证置信级别，在步骤 1640 使用这个置信级别完成验证请求，并且将这些信息从验证引擎 215 转发到事务处理引擎 205 以便包括在发给验证请求人的消息中。

[0247] 上述处理仅是示例性的，并且本领域的技术人员将认识到，不需要以所示的顺序执行步骤，或仅需要执行希望执行的某些步骤，或可以希望这些步骤的各种组合。另外，如果环境允许，可以彼此并行地执行某些步骤，诸如对所提供的每个验证实例的可靠性评估。

[0248] 在本发明的另一个方面，提供了一种方法，以便调整当上述处理产生的验证置信级别不满足提供方或请求验证的另一方所需的信任级别时的条件。在诸如提供的置信级别和所希望的信任级别之间存在差距的情况，授信引擎 110 的操作员处于能够给一方或双方提供机会的位置，以便提供可替换的数据或要求以便缩短信任差距。此处这个处理被称为“信任仲裁”。

[0249] 信任仲裁可以发生在上面参考图 10 和 11 所述的密码验证框架内。如其中所示，提供方或另一方请求与特定事务处理相关联的特定用户的验证。在一种情况下，提供方简单地请求或是肯定的或是否定的验证，并且在从用户处接收适当数据后，授信引擎 110 提供这种二值验证。在诸如这些的情况下，基于授信引擎 110 中设置的偏好确定保证肯定验

证所需的置信程度。

[0250] 然而，还可能提供方可能需要特定的信任级别以便完成特定的事务处理。这种所需的级别可被包括在验证请求中（例如，以98％的置信度验证这个用户），或可由授信引擎110基于与该事务处理相关联的其他因素确定（即，适当地为这个事务处理验证这个用户）。一个这种因素可以是该事务处理的经济价值。对于具有较高经济价值的事务处理，可能需要更高的信任程度。类似地，对于具有高度风险的事务处理，可能需要高的信任程度。相反，对于或是低风险或是低价值的事务处理，提供方或另一个验证请求人可能需要较低的信任级别。

[0251] 信任仲裁处理发生在图10的步骤1050中授信引擎110接收验证数据和图10的步骤1055中将验证结果返回给提供方的步骤之间。在这些步骤之间，如图17所示发生导致信任级别评估和潜在的信任仲裁的处理。在执行简单的二值验证的情况下，图17所示的处理缩减为如上面参考图10所讨论的由事务处理引擎205直接对提供的验证数据和用于标识的用户的登记数据进行比较，将任何差异标记为否定验证。

[0252] 如图17所示，步骤1050中的接收数据之后的第一个步骤是步骤1710中为事务处理引擎205确定这个特定的事务处理的肯定验证所需的信任级别。可以根据若干不同方法中的一个执行这个步骤。可以在进行验证请求时由验证请求人向授信引擎110指出所需的信任级别。验证请求人还可以事先设置存储在仓库210或事务处理引擎205可以访问的其他存储设备内的偏好。每次该验证请求人进行验证请求时可以读取和使用这个偏好。该偏好还可以作为一种安全措施与特定用户相关联，从而总是需要特定的信任级别以便验证该用户，用户偏好存储在仓库210或事务处理引擎205可以访问的其他存储设备内。还可由事务处理引擎205或验证引擎215基于在验证请求中提供的诸如将被验证的事务处理的价值和风险级别的信息推导出所需级别。

[0253] 在一个操作模式中，使用策略管理模块或产生验证请求时使用的其他软件指出该事务处理的验证所需的信任程度。这可用于提供在基于在策略管理模块中指定的策略分配所需级别时将遵从的一系列规则。一种有利的操作模式是将这种模块与提供方的Web服务器相结合，以便适当地确定以提供方的Web服务器发起的事务处理所需的信任级别。以这种方式，可以根据提供方的策略给来自用户的事务处理请求分配所需的信任级别，并且将这种信息与验证请求一起转发到授信引擎110。

[0254] 这种所需的信任级别与提供方想要具有的关于验证的个体事实上是对自身的标识的确定程度相关。例如，如果由于将转手货物，事务处理是提供方需要相当确定程度的事务处理，提供方可以要求85％的信任级别。对于提供方仅验证用户以便允许他观看仅对成员开放的内容或对聊天室行使特权的情况，负面风险可能足够小，从而提供方仅要求60％的信任级别。然而，为了进入好几万美元价值的生产合同，提供方可能要求99％的信任级别或更高。

[0255] 这种所需的信任级别表示对用户必须验证自己以便完成事务处理的度量。如果所需的信任级别例如是85％，用户必须向授信引擎110提供足以使得授信引擎110以85％的置信度认为用户是其所声称的人的验证。这种所需的信任级别和验证置信级别之间的权衡产生肯定的验证（令提供方满意）或信任仲裁的可能。

[0256] 如图17所示，在事务处理引擎205收到所需的信任级别之后，它在步骤1720对所

需的信任级别和验证引擎 215 为当前验证计算的验证置信级别（如参考图 16 讨论的）进行比较。在步骤 1730 如果验证置信级别高于该事务处理的所需信任级别，那么处理进入步骤 1740，其中由事务处理引擎 205 产生针对这个事务处理的肯定的验证。实现这种效果的消息然后被插入验证结果，并且如步骤 1055（见图 10）所示由事务处理引擎 205 返回提供方。

[0257] 然而，如果在步骤 1730 验证置信级别不满足所需信任级别，则对于当前验证存在置信差距，并且在步骤 1750 进行信任仲裁。下面参考图 18 更完整地描述信任仲裁。如下所述这个处理发生在授信引擎 110 的事务处理引擎 205 内。由于不需要验证和其他密码操作以便执行信任仲裁（除了事务处理引擎 205 和其他组件之间的 SSL 通信所需的那些之外），可以在验证引擎 215 之外执行该处理。然而如下所述，任何验证数据的重新评估或其他密码或验证事件将需要事务处理引擎 205 向验证引擎 215 重新提交适当的数据。本领域的技术人员将认识到可以可替换地将信任仲裁构造为部分地或完全发生在验证引擎 215 自身之内。

[0258] 如上所述，信任仲裁是授信引擎 110 在适当的情况下在试图保证肯定的验证时在提供方和用户之间调解协商的处理。如步骤 1805 所示，事务处理引擎 205 首先确定当前情况是否适合信任仲裁。如下面进一步讨论的，这可被基于验证的情况确定，例如，该验证是否已经经过了多轮仲裁，以及基于提供方或用户的偏好确定。

[0259] 在不可能仲裁的情况下，处理进入步骤 1810，其中事务处理引擎 205 产生否定的验证，并且将其插入在步骤 1055 发送给提供方的验证结果内（见图 10）。可有利地用于防止验证不明确地悬置的一种限制是设置从初始验证请求开始的超时时间段。以这种方式，在该时限内未被肯定地验证的任何事务处理被拒绝进一步仲裁并且被否定地验证。本领域发技术人员将认识到这种时限可以根据事务处理的环境以及用户和提供方的希望而改变。还可以对可以进行提供成功验证的尝试的次数做出限制。可由图 5 所述的尝试限制器 535 处理这种限制。

[0260] 如果在步骤 1805 未禁止仲裁，事务处理引擎 205 将投入与事务处理方之一或这两者的协商。如步骤 1820 所示事务处理引擎 205 可以向用户发送消息请求某种形式的附加验证，以便提升产生的验证置信级别。以最简单的形式，这可以简单地指出验证不充分。还可以发送产生一个或多个附加验证实例以便提高验证的整体置信级别的请求。

[0261] 如果用户在步骤 1825 提供了某些附加验证实例，那么事务处理引擎 205 将这些验证实例添加到针对该事务处理的验证数据中，并且如步骤 1015 所示将其转发到验证引擎 215（见图 10），并且基于针对这个事务处理的预先存在的验证实例和新提供的验证实例重新评估验证。

[0262] 可以从授信引擎 110 请求附加类型的验证，以便例如通过电话呼叫进行某种形式的授信引擎 110 操作员（或可信的合作人）和用户之间的人与人接触。可以使用这种电话呼叫或其他非计算机验证提供与个人的人员接触，并且还进行某种形式的基于调查表的验证。这还可以给予检验发起电话号码并且在来访时潜在地进行用户语音分析的机会。即使不能提供附加的验证数据，与用户的电话号码相关联的附加上下文可以提高验证上下文的可靠性。任意修改的数据或基于这个电话呼叫的环境被送入授信引擎 110，以便在考虑验证请求时使用。

[0263] 附加地，在步骤 1820，授信引擎 110 可以给用户提供购买保险的机会，有效地购买更确信的验证。授信引擎 110 的操作员有时可能仅希望在验证的置信级别高于开始的某个阈值的情况下使得可以获得这种选择。实际上，这种用户侧保险是当验证满足授信引擎 110 对验证的通常所需信任级别，但是不满足提供方对这个事务处理的所需信任级别时，授信引擎 110 担保用户的一种方式。以这种方式，即使仅有产生对于授信引擎 110 来说足够的置信度的验证实例，用户仍可以成功地以提供方可能需要的非常高的级别验证。

[0264] 授信引擎 110 的这种功能允许授信引擎 110 为满足授信引擎 110 的验证但是不满足提供方的人担保。这类似于公证人所执行的在文档上增加其签名，以便向稍后阅读该文档的人指出出现在文档上的人实际上是签署它的人的功能。公证人的签名证实用户签署的动作。以相同方式，授信引擎提供进行事务处理的人是他们所声称的人的指示。

[0265] 然而，由于授信引擎 110 人为地提升由用户提供的置信级别，对于授信引擎 110 操作员来说存在较大风险，这是由于用户实际上不满足提供方的所需信任级别。保险的花费被设计为弥补误肯定验证给授信引擎 110（其可以有效地证明用户的验证）带来的风险。用户向授信引擎 110 的操作员支付费用，以便承担以高于实际提供的置信级别验证的风险。

[0266] 由于这种保险系统允许人们从授信引擎 110 购买更高的置信等级，提供方和用户可能都希望在某些事务处理中禁止用户侧保险的使用。提供方可能希望将肯定验证限制为他们知道实际的验证数据支持他们需要的置信程度，并且从而可以指示授信引擎 110 不允许用户侧保险。类似地，为了保护自己的在线身份，用户可能希望禁止为自己使用用户侧保险，或可能希望将其使用局限于不带保险的验证置信级别高于每个界限的情况。这可被用作安全措施以便防止别人偷听口令或偷取智能卡，并且使用它们以低的置信级别进行误验证，然后购买保险产生非常高的（误）置信级别。在确定是否允许用户侧保险时可以评估这些因素。

[0267] 如果用户在步骤 1840 购买保险，则在步骤 1845 基于购买的保险调整验证置信级别，并且在步骤 1730（见图 17）再次比较验证置信级别和所需信任级别。处理从该处继续，并且可以导致步骤 1740 的肯定验证（见图 17）或在步骤 1750 返回信任仲裁处理，以便进一步仲裁（如果允许），或如果禁止进一步仲裁在步骤 1810 的否定验证。

[0268] 除了在步骤 1820 向用户发送消息之外，事务处理引擎 205 还在步骤 1830 向提供方发送消息，指出待决验证当前低于所需的信任级别。该消息还可以给提供方提供如何处理的各种选择。这些选择之一是简单地通知提供方当前的验证置信级别是什么，并且询问提供方是否希望保持当前不能满足的所需信任级别。这可能是有益的，因为在某些情况下，提供方可能具有验证事务处理的独立方法，或可能使用默认的一组要求，其通常导致高于手边特定事务处理实际所需的最初指定的所需级别。

[0269] 例如，标准做法可能是希望与提供方的所有进入购买订单事务处理满足 98％的信任级别。然而，如果最近提供方和长期客户之间以电话讨论了订单，并且之后立刻验证该事务处理，提供方可能仅希望 93％的置信级别，以便简单地降低该事务处理的接受阈值，这是由于电话呼叫有效地给提供方提供了附加的验证。在某些情况下，提供方可能愿意降低其所需的信任级别，但是不是一直到当前的验证置信级别。例如，上面例子中的提供方可以考虑先于订单的电话呼叫可以减少 4％的所需信任程度；然而，这仍然大于用户提供的 93％的置信度。

[0270] 如果提供方不在步骤 1835 调整其所需信任级别，那么在步骤 1730 比较由验证产生的验证置信级别和所需信任级别（见图 17）。如果置信级别现在高于所需信任级别，可以在步骤 1740 在事务处理引擎 205 中产生肯定验证（见图 17）。如果不是，如果允许可以如上所述尝试进一步仲裁。

[0271] 除了请求调整所需信任级别之外，事务处理引擎 205 还可以给请求验证的提供方提供提供方侧保险。这种保险的作用类似于上述用户侧保险。然而此处费用不是相应于授信引擎 110 在验证中超出产生的实际验证置信级别所承担的风险，保险的费用相应于提供方在验证中接受较低信任级别所承担的风险。

[0272] 不是仅降低其实际所需信任级别，提供方可以选择购买保险以便保护自身不受与用户验证中较低的信任级别相关联的附加风险的影响。如上所述，提供方可以有利地仅在已有验证已经高于某个阈值的情况下考虑购买这种保险以弥补信任差距。

[0273] 这种提供方侧保险的可获得性允许提供方选择：或是无自身附加费用地直接降低其信任要求，或是自己承担误验证的风险（基于所需的较低信任级别），或是为验证置信级别和其要求之间的信任差距购买保险，由授信引擎 110 的操作员承担提供的较低置信级别的风险。通过购买保险，提供方有效地保持其高的信任级别要求；由于伪验证的风险被转移到了授信引擎 110 的操作员。

[0274] 如果提供方在步骤 1840 购买保险，在步骤 1730 比较验证置信级别和所需的信任级别（见图 17），并且处理如上所述那样继续。

[0275] 注意还可以用户和提供方这两者响应来自授信引擎 110 的消息。本领域的技术人员将认识到存在可以处理这些情况的多种方法。一种处理多响应的可能性的有利模式是以先到先服务方式对待响应。例如，如果提供方以降低的所需信任级别响应，并且之后用户立刻购买保险提升其自己的验证级别，首先基于来自提供方的降低的信任要求重新评估验证。如果现在验证是肯定的，则忽略用户的保险购买。在另一种有利的操作模式中，仅针对满足新的提供方降低的信任要求所需的保险级别向用户收费（如果即使对于降低的提供方信任要求仍有信任差距）。

[0276] 如果在为验证设置的时限内在步骤 1850 在信任仲裁处理期间未收到来自任意一方的响应，在步骤 1805 重新评估该仲裁。这有效地再次开始仲裁处理。如果时限终止或其他情况阻止步骤 1805 的进一步仲裁，事务处理引擎 205 在步骤 1810 产生否定验证，并且在步骤 1055 返回提供方（见图 10）。如果不是，向用户和提供方发送新消息，并且在需要时重复处理。

[0277] 注意对于某些类型的事务处理，例如，数字签署的不是事务处理的一部分的文档，可以不必有提供方或其他第三方；因此，该事务处理主要在用户和授信引擎 110 之间。在这些情况下，授信引擎 110 具有必须被满足以便产生肯定验证的自己的所需信任级别。然而，在这种情况下，授信引擎 110 通常不希望给用户提供保险以便他能够提升自己签名的置信度。

[0278] 可以使用如上面参考授信引擎 110 所述的各种通信模块执行上面所述和图 16-18 中所示的处理。例如，消息可以是基于 Web 的，并且使用授信引擎 110 和实时下载到在用户或提供方系统上运行的浏览器的小程序之间的 SSL 连接发送。在一种可替换的操作模式中，可由用户和提供方使用便于这种仲裁和保险事务处理的某些专用应用程序。在另一种

可替换的操作模式中，可以使用安全电子邮件操作调解上述仲裁，从而允许推迟的评估和验证的批处理。本领域发技术人员将认识到当适合于环境和提供方的验证要求时可以使用不同的通信模式。

[0279] 下面参考图 19 的描述描述了集成如上所述的本发明的各个方面的示例事务处理。这个例子以授信引擎 110 的调解示出了用户和提供方之间的整个处理。虽然可以使用上面详述的各种步骤和组件执行下面的事务处理，该示出的处理集中于授信引擎 110，用户和提供方之间的交互。

[0280] 当用户在线观看 Web 页面时填写提供方 Web 站点上的订单时，该事务处理在步骤 1900 开始。用户希望向提供方提交以其数字签名签署的这个订单。为了这样做，在步骤 1905 用户将订单与其对签名的请求一起提交给授信引擎 110。用户还提供将如上所述用于验证其身份的验证数据。

[0281] 在步骤 1910，如上所述由授信引擎 110 对验证数据和登记数据进行比较，并且如果产生肯定验证，将以用户的私钥签署的订单的散列与订单自身一起转发到提供方。

[0282] 提供方在步骤 1915 接收签署的订单，然后提供方在步骤 1920 产生关于将要进行的购买的发货清单或其他合同。在步骤 1925 将该合同与对签名的请求一起发送回用户。提供方还在步骤 1930 向授信引擎 110 发送对这个合同事务处理的验证请求，包括由双方签署的合同的散列。为了允许双方数字地签署合同，提供方还包括其自己的验证数据，从而如果需要稍后可以检验合同上提供方的签名。

[0283] 如上所述，授信引擎 110 检验提供方提供的验证数据以便确认提供方的身份，并且如果数据在步骤 1935 产生肯定验证，当从用户处收到数据时继续步骤 1955。如果提供方的验证数据不能以所希望的程度匹配提供方的登记数据，向提供方返回消息请求进一步验证。如上所述，如果需要此处可以执行信任仲裁，以便提供方能够成功地向授信引擎 110 验证自己。

[0284] 当用户在步骤 1940 收到合同时，他对其进行评审，在步骤 1945 产生验证数据以便如果可以接受则签署合同，然后在步骤 1950 将合同的散列和其验证数据发送给授信引擎 110。授信引擎 110 在步骤 1955 检验验证数据，并且如果验证良好，继续如下所述处理合同。如上面参考图 17 和 18 所述，适当时可以执行信任仲裁，以便弥补验证置信级别和该事务处理的所需验证级别之间已有的任意信任差距。

[0285] 授信引擎 110 以用户的私钥签署合同的散列，并且在步骤 1960 将这个签署的散列发送给提供方，其中代表自己签署完整的消息，即，包括以授信引擎 110 的私钥 510 加密的完整消息的散列（包括用户的签名）。由提供方在步骤 1965 接收这个消息。该消息代表签署的合同（使用用户的私钥加密的合同的散列），并且被从授信引擎 110 处接收（使用授信引擎 110 的私钥加密的包括签署的合同的消息的散列）。

[0286] 授信引擎 110 类似地在步骤 1970 以提供方的私钥准备合同的散列，并且将由授信引擎 110 签署的该散列转发给用户。以这种方式，用户还在步骤 1975 接收由提供方签署的合同的拷贝，以及授信引擎 110 签署的对签署的合同的传递的收据。

[0287] 除了上述之外，本发明的一个附加方面提供密码服务提供商模块 (SPM)，客户机侧应用可以使用它作为访问由上述授信引擎 110 提供的功能的手段。提供这种服务的一种有利方法是密码 SPM 调解第三方应用编程接口 (API) 和可以通过网络或其他远程连接访问的

授信引擎 110 之间的通信。下面参考图 20 描述示例的密码 SPM。

[0288] 例如，在典型系统上，程序员可以使用若干 API。每个 API 提供可由运行在系统上的应用程序 2000 做出的一组函数调用。提供适合于密码功能、验证功能和其他安全功能的编程接口的 API 的例子包括由 Microsoft 以其 Windows 操作系统提供的 Cryptographic API(CAPI)2010 和由 IBM、Intel 和其他开放组织成员赞助的 Common Data Security Architecture(CDSA)。将使用 CAPI 作为下面讨论中的示例安全 API。然而，还可将 CDSA 或本领域已知的其他安全 API 用于所述的密码 SPM。

[0289] 当对密码功能进行调用时由用户系统 105 或提供方系统 120 使用这个 API。这些功能可以包括与执行各种密码操作相关联的请求，诸如以特定密钥加密文档、签署文档、请求数字证书、检验签署的文档上的签名以及此处描述的或本领域技术人员已知的其他密码功能。

[0290] 通常在 CAPI 2010 所在的系统上本地地执行这些密码功能。这是由于一般调用的功能需要使用本地用户系统 105 的资源诸如指纹读取器，或使用在本地机器上执行的库编写的软件函数。通常由上面涉及的提供用于执行密码功能的资源的一个或多个服务提供商模块 (SPM)2015，2020 提供对这些本地资源的访问。这些 SPM 可以包括用于执行加密或解密操作的软件库 2015，或能够访问专用硬件 2025 诸如生物测定扫描设备的驱动器和应用程序 2020。在 CAPI 2010 提供可由系统 105 的应用程序 2000 使用的功能的大部分方法中，SPM2015，2020 给 CAPI 提供对与系统上的可用服务相关联的底层功能和资源的访问。

[0291] 根据本发明，可以提供密码 SPM 2030，其能够访问由授信引擎 110 提供的密码功能，并且通过 CAPI 2010 使得应用程序 2000 可获得这些功能。不同于 CAPI 2010 仅能够访问可通过 SPM 2015，2020 本地获得的资源的实施例，此处描述的密码 SPM 2030 能够将对密码操作的请求提交到位于远程的可网络访问的授信引擎 110，以便执行所希望的操作。

[0292] 例如，如果应用程序 2000 需要一种密码操作，诸如签署文档，应用程序 2000 对适当的 CAPI 2010 函数进行函数调用。CAPI 2010 又执行这个函数，使用通过 SPM 2015，2020 和密码 SPM 2030 使其可以获得的资源。在数字签名功能的情况下，密码 SPM 2030 产生将被在通信链路 125 上发送到授信引擎 110 的适当的请求。

[0293] 密码 SPM 2030 和授信引擎 110 之间发生的操作是可能出现在任意其他设备和授信引擎 110 之间的相同操作。然而，通过 CAPI 2010 有效地使得用户系统 105 可获得这些功能，从而它们看似可在用户系统 105 自身上本地获得。然而，不同于普通的 SPM 2015，2020，这些功能被在远程授信引擎 110 上执行，并且响应通信链路 125 上的适当请求将结果传递到密码 SPM 2030。

[0294] 这个密码 SPM 2030 使得用户系统 105 或提供方系统 120 可以获得若干操作，否则这些操作将不可获得。这些功能包括但不限于：文档加密和解密；数字证书颁发；数字签署文档；数字签名的检验；以及本领域技术人员明了的其他操作。

[0295] 在一个不同的实施例中，本发明包括用于对任意数据集合执行本发明的数据保护方法的完整系统。本实施例的计算机系统包括数据分割模块，其包括图 8 所示并且在此处所述的功能。在本发明的一个实施例中，数据分割模块，某些时候在此处被称为安全数据解析器，包括包含数据分割、加密和解密、重新构造或重新组装功能的解析器程序或软件套件。这个实施例还可以包括一个数据存储设施或多个数据存储设施。数据分割模块或安全

数据解析器包括跨平台软件模块套件，其集成在电子基础设施内，或作为需要其数据元素的终极安全的任意应用程序的附件。这种解析处理对任意类型的数据集合，或任意和全部文件类型，或在数据库中对任意行、列或该数据库内的数据单元进行操作。

[0296] 在一个实施例中，可按模块层次方式设计本发明的解析处理，并且任意加密处理适用于本发明的处理。本发明的解析和分割处理的模块层次可以包括但不限于 1) 密码分割，分散并且安全存储在多个位置 ;2) 加密，密码地分割，分散并且安全存储在多个位置 ;3) 加密，密码地分割，加密每一分，然后分散并且安全存储在多个位置 ;和 4) 加密，密码地分割，以不同于第一步骤所使用的加密类型加密每一分，然后分散并且安全存储在多个位置。

[0297] 在一个实施例中，该处理包括根据产生的随机数的内容或密钥分割数据，并且对用于加密将要被保护的数据的分割为解析和分割数据的两个或多个部分或份，并且在一个实施例中，优选地分割为解析和分割数据的四个或多个部分的密钥执行相同的密码分割，对所有部分加密，然后根据请求人对私密性和安全性的要求，分散这些部分并且将其存储回数据库，或将它们重新定位到任意指定的固定的或可移动的设备。可替换地，在另一个实施例中，加密可以发生在分割模块或安全数据解析器的数据集分割之前。被如这个实施例中所述那样处理的原始数据被加密和扰乱并且获得保护。如果希望，加密元素的散布实际上可以在任何位置，包括但不限于，单个服务器或数据存储设备，或在分离的数据存储设施或设备之间。在一个实施例中加密密钥管理可以包括在软件套件内，或在另一个实施例中，可被集成在已有的基础设施内或任意其他所希望的位置。

[0298] 密码分割 (cryptosplit) 将数据划分为 N 份。划分可以基于任意大小的数据单元，包括单个位，多个位，字节，千字节，兆字节，或更大的单元，以及预定的或随机产生的数据单元大小的任意模式或组合。该单元还可以具有基于一组随机或预定值的不同大小。这意味着数据可被看成这些单元的一个序列。以这种方式，例如通过使用一个或多个预定或随机产生的模式、序列或数据单元大小的组合，数据单元自身的大小可以致使数据更安全。然后这些单元（随机地或通过预定的一组值）被分配到 N 份。这个分配还涉及混淆份中所述单元的顺序。本领域的普通技术人员容易明了，可以根据多种可能的选择这些将数据单元分配到份中，包括但不限于固定大小，预定大小，或预定或随机产生的数据单元大小的一个或多个组合、模式或序列。

[0299] 密码分割处理或 cryptosplit 的一个例子考虑 23 个字节大小的数据，数据单元大小被选择为 1 字节，并且份数被选择为 4。每个字节将被分配到 4 份中的一份内。假设随机分配，获得一个密钥以创建一系列 23 个随机数 (r1,r2,r3 到 r23)，每个具有相应于 4 个份的 1 到 4 之间的值。每个数据单元（在这个例子中 23 个单独的数据字节）与相应于 4 份之一的 23 个随机数之一相关联。可以通过将数据的第一字节置于份数 r1，字节 2 置于份数 r2，字节 3 置于份数 r3，直到将数据的第 23 个字节置于份数 r23，发生将数据字节分配到 4 份中。本领域的普通技术人员容易明了，在本发明的密码分割处理中可以使用多种其他可能的步骤或步骤的组合或序列，包括数据单元的大小，并且上述例子是对密码分割数据的一个处理的非限制性描述。为了重新创建原始数据，将执行相反的操作。

[0300] 在本发明的密码分割处理的另一个实施例中，一种密码分割处理的选择是在份中提供足够的冗余，从而仅需要这些份的一个子集，以便将数据重新组装或恢复为其原始或

可用形式。作为非限制性例子，可按“3of4”密码分割进行密码分割，从而仅需要 4 份中的 3 份将数据重新组装或恢复为其原始或可用形式。这也称为“M of N 密码分割”，其中 N 是总份数，M 至少比 N 小 1。本领域的普通技术人员容易明了，存在在本发明的密码分割处理中创建这种冗余的许多可能。

[0301] 在本发明的密码分割处理的一个实施例中，每个数据单元被存储在两个份 - 主份和备用份中。使用上述的“3of4”密码分割处理，可以丢失任意一份，并且由于仅需要总共 4 份中的 3 份，足以用未丢失的数据单元重新组装或恢复原始数据。如此处所述，产生相应于所述份之一的随机数。该随机数被与一个数据单元相关联，并且被基于一个密钥存储在相应的份内。在这个实施例中，使用一个密钥产生主和备份份随机数。如此处针对本发明的密码分割处理所描述的，产生等于数据单元数目的从 0 到 3 的一组随机数（还称为主份数）。然后产生等于数据单元数目的从 1 到 3 的另一组随机数（还称为备份份数）。数据的每个单元然后被与主份数和备份份数相关联。可替换地，可以产生少于数据单元数目的一组随机数，并且重复该随机数集合，但是这将减少敏感数据的安全性。主份数用于确定数据单元被存储在哪个份内。备份份数被与主份数组合，以便创建 0 和 3 之间的第三份数，并且这个数字用于确定将数据单元存储在哪个份内。在这个例子中，确定第三份数的等式为：

[0302] （主份数 + 备份份数）MOD 4 = 第三份数

[0303] 在上述实施例中，主份数为 0 和 3 之间并且备份份数在 1 和 3 之间确保第三份数与主份数不同。这导致将数据单元存储在两个不同的份内。本领域的普通技术人员容易明了，除了此处公开的实施例之外，存在许多执行冗余密码分割和非冗余密码分割的方法。例如，可以使用不同的算法混淆每个份内的数据单元。例如，可以在将原始数据分割为数据单元时，或在将数据单元放置在份内之后，或在份充满之后执行这种数据单元混淆。

[0304] 可以对任意大小的数据单元执行此处描述的各种密码分割处理和数据混淆处理，以及本发明的密码分割和数据混淆方法的所有其他实施例，包括但不限于：小至单个位，多个位，字节，千字节，兆字节或更大。

[0305] 执行此处描述的密码分割处理的一个源码实施例的例子为：

[0306] DATA[1 :24]- 将被分割的数据的字节阵列

[0307] SHARES[0 :3 ;1 :24]- 二维矩阵，每一行表示一个份

[0308] RANDOM[1 :24]- 在范围 0..3 内的阵列随机数

[0309] S1 = 1 ;

[0310] S2 = 1 ;

[0311] S3 = 1 ;

[0312] S4 = 1 ;

[0313] For J = 1 to 24 do

[0314] Begin

[0315] IF RANDOM[J[ == 0then

[0316] Begin

[0317] SHARES[1,S1] = DATA[J] ;

[0318] S1 = S1+1 ;

[0319] End

[0320] ELSE IF RANDOM[J[ == 1then

[0321] Begin

[0322] SHARES[2,S2] = DATA[J] ;

[0323] S2 = S2+1 ;

[0324] END

[0325] ELSE IF RANDOM[J[ == 2then

[0326] Begin

[0327] Shares[3,S3] = data[J] ;

[0328] S3 = S3+1 ;

[0329] End

[0330] Else begin

[0331] Shares[4,S4] = data[J] ;

[0332] S4 = S4+1 ;

[0333] End ;

[0334] END ;

[0335] 执行此处描述的密码分割 RAID 处理的一个源码实施例的例子为 :

[0336] 产生两组数,PrimaryShare 为 0 到 3,BackupShare 为 1to3。然后以与上述的密码分割相同的处理,将每个数据单元放入 share[primaryshare[1]] 和 share[(primaryshare[1]+backupshare[1])mod 4。该方法可被扩缩至任意大小 N,其中仅需要 N-1 份以便恢复数据。

[0337] 加密的数据元素的检索,重新组合,重新组装或重新构造可以利用任意数目的验证技术,包括但不限于 :诸如指纹识别的生物测定,脸部扫描,手扫描,虹膜扫描,视网膜扫描,耳朵扫描,血管模式识别,或 DNA 分析。如果希望,本发明的数据分割和 / 或解析器模块可被集成在各种基础设施产品或应用中。

[0338] 本领域已知的传统加密技术依赖于一个或多个密钥,所述密钥用于加密该数据并且使其在没有该密钥的情况下是不可使用的。然而,数据保持完整无缺并且易受攻击。在一个实施例中,通过执行加密文件的密码解析和分割为两个或多个部分或份,并且在另一个实施例中优选地四个或更多份,对每份数据增加另一层加密,然后在不同的物理和 / 或逻辑位置存储这些份,本发明的安全数据解析器解决了这个问题。当使用可移动设备诸如数据存储设备,或是通过将一个或多个数据份置于另一方的控制下,将份物理地移出系统时,有效地排除了危及受保护的数据的任意可能。

[0339] 图 21 中示出并且在下面描述了本发明的安全数据解析器的一个实施例的例子以及如何利用它的例子。然而,本领域的普通技术人员容易明了,除了下面非限制性的例子之外,可以用各种方式使用本发明的安全数据解析器。作为一种部署选择并且在一个实施例中,可以带有外部会话密钥管理或会话密钥的安全内部存储实现安全数据解析器。在实现上,产生用于保护应用程序和加密目的的解析器主密钥。还应当注意,将解析器主密钥结合在获得的受保护数据内允许由工作组、企业或延及的人员 (extended audience) 内的个体分享受保护数据的灵活性。

[0340] 如图 21 所示,本发明的这个实施例示出了由安全数据解析器对数据执行的与解

析的数据一起存储会话主密钥的处理的步骤：

[0341] 1. 产生会话主密钥，并且使用 RS1 流码加密数据。

[0342] 2. 根据会话主密钥的模式，将获得的加密数据划分为解析数据的 4 份或部分。

[0343] 3. 在该方法的这个实施例中，将会话主密钥和受保护的数据份一起存储在数据仓库中。根据解析器主密钥的模式划分会话主密钥，并且将密钥数据附加到加密的解析数据上。

[0344] 4. 获得的 4 份数据包含原始数据的加密部分以及会话主密钥的部分。为 4 个数据份中的每一个产生流码密钥。

[0345] 5. 加密每一份，然后将加密密钥存储在与加密的数据部分或份不同的位置：份 1 得到密钥 4，份 2 得到密钥 1，份 3 得到密钥 2，份 4 得到密钥 3。

[0346] 为了恢复原始数据格式，反转上述步骤。

[0347] 本领域的普通技术人员容易明了，如果希望，可以按不同的顺序或可以多次重复执行此处描述的方法的某些步骤。本领域技术人员还容易明了可以彼此不同地处理数据的各个部分。例如，可以仅对解析的数据的一个部分执行多个解析步骤。只要数据可被重新组装，重新构造，重整，解密或恢复为其原始或其他可用形式，可以用任意所希望的方法唯一地保护解析数据中的每一部分。

[0348] 如图 22 所示并且如此处所述，本发明的另一个实施例包括由安全数据解析器对数据执行的用于将会话主密钥存储在一个或多个分离的密钥管理表内的处理的步骤：

[0349] 1. 产生会话主密钥，并且使用 RS1 流码加密数据。

[0350] 2. 根据会话主密钥的模式，将获得的加密数据划分为解析数据的 4 份或部分。

[0351] 3. 在该方法的这个实施例中，将会话主密钥存储在数据仓库中的单独的密钥管理表内。产生这个事务处理的唯一事务处理 ID。将事务处理 ID 和会话主密钥存储在单独的密钥管理表内。根据解析器主密钥的模式划分事务处理 ID，并且将该数据附加到加密的解析或划分数据上。

[0352] 4. 获得的 4 份数据包含原始数据的加密部分以及事务处理 ID 部分。

[0353] 5. 为 4 份数据中的每一份产生流码密钥。

[0354] 6. 加密每一份，然后将加密密钥存储在与加密的数据部分或份不同的位置：份 1 得到密钥 4，份 2 得到密钥 1，份 3 得到密钥 2，份 4 得到密钥 3。

[0355] 为了恢复原始数据格式，反转上述步骤。

[0356] 本领域的普通技术人员容易明了，如果希望，可以按不同的顺序或可以多次重复执行此处描述的方法的某些步骤。本领域技术人员还容易明了可以彼此不同地处理数据的各个部分。例如，可以仅对解析的数据的一个部分执行多个划分或解析步骤。只要数据可被重新组装，重新构造，重整，解密或恢复为其原始或其他可用形式，可以用任意所希望的方法唯一地保护解析数据的每一部分。

[0357] 如图 23 所示，本发明的这个实施例示出了由安全数据解析器对数据执行的用于与解析数据一起存储会话主密钥的处理的步骤：

[0358] 1. 存取与经验证的用户相关联的解析器主密钥。

[0359] 2. 产生唯一的会话主密钥。

[0360] 3. 根据解析器主密钥和会话主密钥的异或函数导出中间密钥。

[0361] 4. 以中间密钥为密钥，使用已有或新的加密算法可选择地加密数据。

[0362] 5. 根据中间密钥的模式，将获得的可选择地加密的数据划分为解析数据的 4 份或部分。

[0363] 6. 在该方法的这个实施例中，将会话主密钥与受保护的数据份一起存储在数据仓库内。根据解析器主密钥的模式划分会话主密钥，并且将密钥数据附加到可选择地加密的解析数据上。

[0364] 7. 获得的多份数据包含原始数据的可选择地加密的部分以及会话主密钥的部分。

[0365] 8. 可选择地为 4 份数据中的每一份产生加密密钥。

[0366] 9. 可选择地以已有或新的加密算法加密每一份，然后将加密密钥存储在与加密的数据部分或份不同的位置：例如，份 1 得到密钥 4，份 2 得到密钥 1，份 3 得到密钥 2，份 4 得到密钥 3。

[0367] 为了恢复原始数据格式，反转上述步骤。

[0368] 本领域的普通技术人员容易明了，如果希望，可以按不同的顺序或可以多次重复执行此处描述的方法的某些步骤。本领域技术人员还容易明了可以彼此不同地处理数据的各个部分。例如，可以仅对解析的数据的一个部分执行多个解析步骤。只要数据可被重新组装，重新构造，重整，解密或恢复为其原始或其他可用形式，可以用任意所希望的方法唯一地保护解析数据的每一部分。

[0369] 如图 24 所示并且如此处所述，本发明的另一个实施例包括由安全数据解析器对数据执行的用于将会话主密钥存储在一个或多个分离的密钥管理表内的处理的步骤：

[0370] 1. 存取与经验证的用户相关联的解析器主密钥。

[0371] 2. 产生唯一的会话主密钥。

[0372] 3. 根据解析器主密钥和会话主密钥的异或函数导出中间密钥。

[0373] 4. 以中间密钥为密钥，使用已有或新的加密算法可选择地加密数据。

[0374] 5. 根据中间密钥的模式，将获得的可选择地加密的数据划分为解析数据的 4 份或部分。

[0375] 6. 在该方法的这个实施例中，将会话主密钥存储在数据仓库中的分离的密钥管理表内。产生这个事务处理的唯一事务处理 ID。将事务处理 ID 和会话主密钥存储在单独的密钥管理表内，或将会话主密钥和事务处理 ID 传回调用程序以便进行外部管理。根据解析器主密钥的模式划分事务处理 ID，并且将该数据附加到加密的解析或划分数据上。

[0376] 7. 获得的 4 份数据包含原始数据的可选择地加密的部分以及事务处理 ID 的部分。

[0377] 8. 可选择地为 4 份数据中的每一份产生加密密钥。

[0378] 9. 可选择地加密每一份，然后将加密密钥存储在与加密的数据部分或份不同的位置：例如，份 1 得到密钥 4，份 2 得到密钥 1，份 3 得到密钥 2，份 4 得到密钥 3。

[0379] 为了恢复原始数据格式，反转上述步骤。

[0380] 本领域的普通技术人员容易明了，如果希望，可以按不同的顺序或可以多次重复执行此处描述的方法的某些步骤。本领域技术人员还容易明了可以彼此不同地处理数据的各个部分。例如，可以仅对解析的数据的一个部分执行多个划分或解析步骤。只要数据可被重新组装，重新构造，重整，解密或恢复为其原始或其他可用形式，可以用任意所希望的方法唯一地保护解析数据的每一部分。

[0381] 本领域的普通技术人员容易明了，各种加密方法适用于本发明的方法。One Time Pad 算法通常被认为是最安全的加密方法之一，并且适用于本发明的方法。使用 One Time Pad 算法需要产生与将被保护的数据一样长的密钥。在某些情况下可能不太希望使用这个方法，诸如由于将被保护的数据集的大小导致产生和管理非常长的密钥的情况。在 One Time Pad(OTP) 算法中，使用简单的异或。对于相同长度的两个二进制流 x 和 y，x XOR y 意味着 x 和 y 的位异或。

[0382] 在位的级别产生：

[0383] 0 XOR 0 = 0

[0384] 0 XOR 1 = 1

[0385] 1 XOR 0 = 1

[0386] 1 XOR 1 = 0

[0387] 此处针对将被分割的 n 字节秘密 s（或数据集）描述这个处理的例子。该处理将产生 n 字节的随机值 a，并且然后设置：

[0388] b = a XOR s

[0389] 注意可以通过下面的等式导出“s”：

[0390] s = a XOR b

[0391] a 和 b 的值被称为份或部分，并且被放置在分离的仓库中。一旦秘密 s 被分割为两个或多个份，它将被以安全的方式丢弃。

[0392] 本发明的安全数据解析器可以利用这个功能，执行结合多个不同秘密密钥值：K1，K2，K3，Kn，K5 的多个 XOR 函数。在该操作的开始，对将被保护的数据进行第一加密操作，安全数据＝数据 XOR 秘密密钥 5：

[0393] S = D XOR K5

[0394] 为了例如在 4 份 S1，S2，S3，Sn 中安全地存储获得的加密数据，根据 K5 的值将该数据解析和分割为“n”段或份。这个操作导致原始加密数据的“n”个伪随机份。可以用剩余的秘密密钥值对每一份执行后续的 XOR 函数，例如：安全数据分段 1 ＝加密的数据份 1XOR 秘密密钥 1：

[0395] SD1 = S1 XOR K1

[0396] SD2 = S2 XOR K2

[0397] SD3 = S3 XOR K3

[0398] SDn = Sn XOR Kn

[0399] 在一个实施例中，可能不希望任意一个仓库包含足够的信息以便解密保持的信息，从而将解密该份所需的密钥存储在不同的数据仓库内：

[0400] Depository 1：SD1，Kn

[0401] Depository 2：SD2，K1

[0402] Depository 3：SD3，K2

[0403] Depository n：SDn，K3

[0404] 另外，可将检索原始会话加密密钥 K5 所需的信息附加到每个份。因此，在此处描述的密钥管理例子中，以根据与安装相关的解析器主密钥 (TID1，TID2，TID3，TIDn) 分割为“n”份的事务处理 ID 引用原始会话主密钥：

[0405] Depository 1 :SD1, Kn, TID1

[0406] Depository 2 :SD2, K1, TID2

[0407] Depository 3 :SD3, K2, TID3

[0408] Depository n :SDn, K3, TIDn.

[0409] 在此处所述的结合的会话密钥例子中，根据与安装相关的解析器主密钥 (SK1, SK2, SK3, SKn) 的内容将会话主密钥分割为“n”份 :

[0410] Depository 1 :SD1, Kn, SK1

[0411] Depository 2 :SD2, K1, SK2

[0412] Depository 3 :SD3, K2, SK3

[0413] Depository n :SDn, K3, SKn.

[0414] 除非检索全部 4 份，根据这个例子不能重新组装数据。即使捕获了全部 4 份，在不能访问会话主密钥和解析器主密钥的情况下，也不可能重新组装或恢复原始信息。

[0415] 这个例子已经描述了本发明的方法的一个实施例，并且还在另一个实施例中描述了用于将份放置在仓库中，从而可以组合所有仓库中的份以便形成保密验证材料的算法。所需的计算非常简单并且快速。然而，采用 One Time Pad(OTP) 算法，由于密钥大小与被存储的数据的大小相同，可能存在使其不太合意的情况，诸如保护大的数据集。因此，可能需要存储和传输大约两倍于原始数据的数量，在某些情况下这是不希望的。

[0416] 流码 RS1

[0417] 流码 RS1 分割技术非常类似于此处描述的 OTP 分割技术。取代 n 字节随机值，产生 n’ = min(n,16) 字节的随机值，并且用于作为 RS1 流码算法的密钥。RS1 流码算法的优点是从非常小的种子数产生伪随机密钥。另外在不危及安全性的情况下，RS1 流码算法加密的执行速度被认为是现有技术中公知的三重 DES 加密的速度的大约 10 倍。RS1 流码算法是本领域公知的，并且可被用于产生在 XOR 函数中使用的密钥。RS1 流码算法可以与其他商业可获得的流码算法互操作，诸如 RSA Security 公司的 RC4™ 流码算法，并且适用于本发明的方法。

[0418] 使用上面的密钥符号，K1 到 K5 现在是 n 字节的随机值，并且设置 :

[0419] SD1 = S1 XOR E(K1)

[0420] SD2 = S2 XOR E(K2)

[0421] SD3 = S3 XOR E(K3)

[0422] SDn = Sn XOR E(Kn)

[0423] 其中 E(K1) 到 E(Kn) 是以 K1 到 Kn 为密钥的 RS1 流码算法的输出的前 n 个字节。如此处所述，份现在被放置在数据仓库内。

[0424] 在这个流码 RS1 算法中，所需的计算近似与 OTP 算法一样简单且快速。使用 RS1 流码的这个例子的益处是系统仅需要存储和传输多于每份要保护的原始数据的大小的平均大约 16 个字节。当原始数据的大小多于 16 字节时，这种 RS1 算法比 OTP 算法更有效，这简单地是由于它更短。本领域的普通技术人员容易明了各种加密方法或算法适用于本发明，包括但不限于 RS1, OTP, RC4™, Triple DES 和 AES。

[0425] 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存在多个主要优点。一个优点是得自于将数据的份移动到可以位于不同的逻辑、物理或地理位置的一个或多个数

据仓库或存储设备上的不同位置的安全性。当例如物理地分割数据的份并且置于不同人员的控制下时，极大地减小了危及数据安全的可能性。

[0426] 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用于保护数据的方法的步骤，以提供保持敏感数据安全性的综合处理。使用安全密钥加密数据，并且根据该安全密钥将其分割为一个或多个份，并且在一个实施例中分割为 4 份。以被根据一个安全密钥保护在 4 个份内的引用指针安全地存储安全密钥。单独加密数据份，并且将密钥安全地存储在不同的加密的份。当被组合时，根据此处公开的方法的用于保护数据的整个处理成为用于数据安全的综合程序包 (package)。

[0427] 根据本发明的方法保护的数据可被容易地检索和恢复，重新组成，重新组装，解密或返回其原始或其他适合使用的形式。为了恢复原始数据，可以利用下面的项目 ：

[0428] 1. 数据集的所有份或部分。

[0429] 2. 再现用于保护该数据的方法的处理流的知识和能力。

[0430] 3. 访问会话主密钥。

[0431] 4. 访问解析器主密钥。

[0432] 因此，可能希望规划安全安装，其中上述元素中的至少一个可以被物理地与系统的其余组件分离（例如在不同的系统管理员的控制下）。

[0433] 可以通过使用解析器主密钥增强调用数据安全方法应用程序的对抗诈骗应用程序的保护。在采取任意活动之前，在本发明的这个实施例中可能需要安全数据解析器和该应用程序之间的互验证握手。

[0434] 系统的安全性要求不存在用于重建原始数据的“后门”方法。对于可能产生数据恢复问题的装置，可以增强安全数据解析器以便提供所述 4 个份和会话主密钥仓库的镜像。诸如 RAID（用于将信息分散在若干盘上的廉价盘冗余阵列）的硬件选择和诸如复制的软件选择也可以帮助数据恢复规划。

[0435] 密钥管理

[0436] 在本发明的一个实施例中，数据保护方法使用用于加密操作的三组密钥。基于安装，每组密钥可以具有单独的密钥存储、检索、安全性和恢复选择。可以使用的密钥包括但不限于 ：

[0437] 解析器主密钥

[0438] 这个密钥是与安全数据解析器的安装相关联的单个密钥。其被安装在其上部署了安全数据解析器的服务器上。存在适用于保护这个密钥的各种选择，包括但不限于 ：例如，智能卡，单独的硬件密钥存储，标准密钥存储，定制密钥存储，或在受保护的数据库表内。

[0439] 会话主密钥

[0440] 每次保护数据时可以产生会话主密钥。会话主密钥用于在解析和分割操作之前加密数据。它还可被作为解析加密数据的一种装置结合（如果会话主密钥未被集成在解析数据内）。可以用各种方式保护会话主密钥，包括但不限于，例如标准密钥存储，定制密钥存储，单独的数据库表，或保护在加密的份内。

[0441] 份加密密钥

[0442] 对于创建的数据集的每一份或几部分，可以产生单独的份加密密钥以便进一步加密该份。份加密密钥可被存储在与被加密的份不同的份内。

[0443] 本领域的普通技术人员容易明了，本发明的数据保护方法和计算机系统广泛地适用于任意设置或环境中的任意类型的数据。除了在 Internet 上或在顾客和提供方之间进行的商业应用之外，本发明的数据保护方法和计算机系统可高度适用于非商业或私有设置或环境。可以使用此处描述的方法和系统保护希望相对于任意未授权用户受到保护的任意数据集。例如，通过采用用于保护数据的本发明的方法和系统，可以有利地将对公司或组织内的特定数据库的访问仅局限到选择的用户。另一个例子是文档的产生，修改或访问，其中希望限制访问或阻止未授权或意外访问或一组选择的个体、计算机或工作站之外的公开。本发明的数据保护方法和系统被应用于任意非商业或商业环境或任意设置的设置的这些和其他例子包括但不限于任意组织、政府机构或公司。

[0444] 在本发明的另一个实施例中，数据保护方法使用用于加密操作的三组密钥。基于安装，每组密钥可以具有单独的密钥存储、检索、安全性和恢复选择。可以使用的密钥包括但不限于：

[0445] 1. 解析器主密钥

[0446] 这个密钥是与安全数据解析器的安装相关联的单个密钥。它被安装在其上部署了安全数据解析器的服务器上。存在适用于保护这个密钥的各种选择，包括但不限于：例如，智能卡，单独的硬件密钥存储器，标准密钥存储器，定制密钥存储器，或在受保护的数据库表内。

[0447] 2. 会话主密钥

[0448] 每次保护数据时可以产生会话主密钥。结合解析器主密钥使用会话主密钥以便导出中间密钥。可以用各种方式保护会话主密钥，包括但不限于，例如标准密钥存储器，定制密钥存储器，单独的数据库表，或保护在加密的份内。

[0449] 3. 中间密钥

[0450] 每次保护数据时可以产生中间密钥。中间密钥用于在解析和分割操作之前加密数据。它还可被作为解析加密数据的装置结合。

[0451] 份加密密钥

[0452] 对于创建的数据集的每一份或几部分，可以产生单独的份加密密钥以便进一步加密该份。份加密密钥可被存储在与被加密的份不同的份内。

[0453] 本领域的普通技术人员容易明了，本发明的数据保护方法和计算机系统广泛地适用于任意设置或环境中的任意类型的数据。除了在 Internet 上或在顾客和提供方之间进行的商业应用之外，本发明的数据保护方法和计算机系统可高度适用于非商业或私人设置或环境。可以使用此处描述的方法和系统保护希望相对于任意未授权用户受到保护的任意数据集。例如，通过采用用于保护数据的本发明的方法和系统，可以有利地将对公司或组织内的特定数据库的访问仅局限到选择的用户。另一个例子是文档的产生、修改或访问，其中希望限制访问或阻止未授权或意外访问或一组选择的个体、计算机或工作站之外的公开。本发明的数据保护方法和系统适用于任意非商业或商业环境或任意设置的设置，包括但不限于，任意组织，政府机构或公司的方式的这些和其他例子。

[0454] 工作组，工程，单个 PC/ 膝上计算机或跨平台数据安全

[0455] 本发明的数据保护方法和计算机系统还可用于工作组，工程，单个 PC/ 膝上计算机，以及在例如商业、办公室、政府机构中使用的任意其他平台，或创建、处理或存储敏感数

据的任意设置的数据保护。本发明提供了已知被诸如美国政府的组织所追求的在整个政府组织或州或联邦级别政府之间实现的用于保护数据的方法和计算机系统。

[0456] 本发明的数据保护方法和计算机系统提供了不仅能够解析和分割平坦文件，而且能够解析和分割数据字段、集合和/或任意类型的表的能力。另外，能够在这个处理下保护所有形式的数据，包括但不限于，文本，视频，图像，生物测定和语音数据。本发明的数据保护方法的可伸缩性，速度和数据吞吐率仅受用户有权支配的硬件的限制。

[0457] 在本发明的一个实施例中，如下所述在工作组环境中利用该数据保护方法。在一个实施例中，如图 23 所示并且如下所述，本发明的工作组级数据保护方法使用 TrustEngine 的私钥管理功能，以便存储用户/组关系和一组用户共享安全数据所必须的相关私钥（解析器组主密钥）。取决于如何部署解析器主密钥，本发明的方法具有保护企业、工作组或个体用户的数据的能力。

[0458] 在一个实施例中，可以提供附加的密钥管理和用户/组管理程序，使得能够实现具有单个管理和密钥管理点的大规模工作组。由单个维护程序处理密钥产生，管理和撤销，随着用户数目的增加，全部这些将变得尤其重要。在另一个实施例中，还可以通过一个或几个不同的系统管理员建立密钥管理，在需要时这可以不允许任意一个人和组控制数据。这允许按由组织定义的角色、责任、成员资格、权利等获得对受保护数据的管理，并且可将对受保护数据的访问限制到仅为被允许或需要的人以便仅能访问其所工作的部分，而其他人诸如管理人或执行人可以访问所有受保护的数据。这个实施例允许在公司或组织内不同组之间共享受保护的数据，而同时仅允许某些选择的个人，诸如具有授权和预定角色和责任的人观看整体数据。另外，本发明的方法和系统的实施例还允许在例如需要某种共享但可能不是允许任意一方访问所有数据的不同公司，或公司的不同部门或单位，或任意不同的组织部门，团体，机构，或任意政府或组织或任意类型的办公室等之间共享数据。对本发明的这种方法和系统的需求和利用的特定明显例子是例如在政府区域、机构和办公室之间，以及在大型公司或任意其他组织的不同单位、部门或办公室之间允许共享但是保持安全性。

[0459] 本发明的方法在较小规模上的适用性的例子如下。将解析器主密钥用作安全数据解析器对于组织的序列化或印记 (branding)。当对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时，此处描述的数据保护方法被用于在用户组内共享文件。

[0460] 在图 25 所示并且在下面所述的例子中，存在 6 个用户，他们被定义有组织内的头衔或角色。侧条表示用户根据其角色可能所属的 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。

[0461] 当为在这个例子中的使用配置安全数据解析器时，系统管理员通过维护程序从操作系统中访问用户和组信息。这个维护程序基于用户在组中的成员资格产生并且给用户分配解析器组主密钥。

[0462] 在这个例子中，高级职员组中有三个成员。对于这个组，活动是：

[0463] 1. 访问高级职员组的解析器组主密钥（如果不可获得则产生密钥）；

[0464] 2. 产生将 CEO 与高级职员组相关联的数字证书；

[0465] 3. 产生将 CFO 与高级职员组相关联的数字证书；

[0466] 4. 产生将副总裁、销售与高级职员组相关联的数字证书。

[0467] 可以为每个组和每个组内的每个成员进行相同组活动。当维护程序完成时，解析器组主密钥成为组的每个成员的共享凭证。当通过维护程序将用户从组中删除时，可以自动地进行分配的数字证书的撤销，而不会影响组中的其余成员。

[0468] 一旦定义了共享凭证，解析和分割处理保持相同。当要保护文件，文档或数据元素时，提示用户保护该数据时所使用的目标组。获得的受保护的数据仅可由该目标组的其他成员访问。本发明的方法和系统的这种功能可被用于任意其他计算机系统或软件平台，并且可被例如集成到已有的应用程序中，或为了文件安全单独使用。

[0469] 本领域的普通技术人员任意明了，任意一个加密算法或加密算法组合适用于本发明的方法和系统。例如，在一个实施例中，可以重复加密步骤以便产生多层加密方案。另外，可以在重复的加密步骤中使用不同的加密算法或加密算法组合，从而将不同的加密算法应用于多层加密方案的不同层。这样，加密方案本身可以成为用于针对未授权使用或访问保护敏感数据的本发明的方法的一个组成部分。

[0470] 可以作为内部组件、作为外部组件、或作为错误检测组件包括安全数据解析器。例如，在一种适合的方法中，当使用根据本发明的安全数据解析器创建数据的多个部分，以便确保一个部分内的数据的完整性时，在该部分内以预定的间隔取散列值，并且将其附加到该间隔的末尾。该散列值是数据的可预测并且可再现的数字表示。如果数据中任意位发生改变，该散列值将不同。扫描模块（作为安全数据解析器之外的独立组件或作为安全数据解析器的内部组件）可以扫描由安全数据解析器产生的数据的所述部分。将数据的每个部分（或可替换地，根据某个间隔，或通过随机或伪随机采样，不是数据的所有部分）与附加的散列值或多个值进行比较，并且可以采取一种动作。该动作可以包括对匹配或不匹配的值的报告，对不匹配的值的报警，或调用某个外部或内部程序以便触发数据恢复。例如，可以基于这样的概念通过调用恢复模块执行数据恢复，即，根据本发明可能不是需要所有部分以产生原始数据。

[0471] 可以使用附加到所有数据部分或数据部分的子集内的任意位置的任意适合的完整性信息实现任意其他适合的完整性检查。完整性信息可以包括可用于确定数据部分的完整性的任意适合的信息。完整性信息的例子可以包括基于任意适合的参数计算的散列值（例如，基于各个数据部分），数字签名信息，消息验证码（MAC）信息，任意其他适合的信息，或其任意组合。

[0472] 本发明的安全数据解析器可用于任意适合的应用中。即，此处描述的安全数据解析器具有不同计算领域和技术中的各种应用。下面讨论几个这种领域。应当理解这些仅是说明的性质，并且任意其他适合的应用可以使用该安全数据解析器。还应当理解，描述的例子仅是说明性的实施例，可以用任意适合的方式对其进行修改以便满足任意适合的要求。例如，解析和分割可以基于任意适合的单元，诸如按位、按字节、按千字节、按兆、按其任意组合、或按任意其他适合的单元。

[0473] 本发明的安全数据解析器可用于实现安全物理标记，从而可以请求存储在物理标记中的数据，以便访问存储在另一个存储区域内的附加数据。在一种适合的方法中，物理标记，诸如小型 USB 闪存驱动器、软盘、光盘、智能卡、或任意其他适合的物理标记可被用于存储根据本发明的解析数据的至少两个部分中的一个部分。为了访问原始数据，需要访问该 USB 闪存驱动器。因此，在可以访问原始数据之前，保持解析数据的一个部分的个人计算机

需要附加具有解析数据的另一部分的USB闪存驱动器。图26示出了这种应用。存储区域2500包括解析数据的一个部分2502。需要使用任意适合的通信接口2508(例如，USB，串行，并行，蓝牙，红外线，IEEE 1394，以太网或任意其他适合的通信接口）将具有解析数据的一个部分2506的物理标记2504连接到存储区域2500，以便访问原始数据。这在敏感数据单独保留在计算机上，并且易遭受未授权访问尝试的情况下是有用的。通过移去物理标记（例如，USB闪存驱动器），不可访问敏感数据。应当理解，可以使用用于使用物理标记任意其他适合方法。

[0474] 本发明的安全数据解析器可用于实现安全验证系统，从而使用安全数据解析器解析和分割用户的登记数据（例如，口令、私人加密密钥、指纹样板、生物测定数据或任意其他适合的用户登记数据）。可以解析和分割用户登记数据，从而将其一个或多个部分存储在智能卡、政府通用访问卡、任意适合的物理存储设备（例如，磁或光盘、USB钥匙驱动器等）或任意其他适合设备上。解析的用户登记数据一个或多个其他部分可被存储在执行验证的系统上。被解析的用户登记数据的一个或多个部分可以被存储在执行验证的系统中。这给验证处理提供了附加级别的安全性（例如，除了从生物测定来源获得的生物测定验证信息之外，还必须通过适当的解析和分割数据部分获得用户登记数据）。

[0475] 本发明的安全数据解析器可被集成到任意适合的已有系统内，以便在每个系统的相应环境中提供对其功能的使用。图27示出了示例系统2600的方框图，其可以包括软件，硬件或用于实现任意适合应用的这两者。系统2600可以是已有系统，其中安全数据解析器2602可被改进为集成组件。可替换地，安全数据解析器2602可被例如在其最早设计阶段集成到任意适合的系统2600内。安全数据解析器2602可被集成到系统2600的任意适合级别。例如，安全数据解析器2602可被集成在充分后端级别，从而安全数据解析器2602的存在对于系统2600的端用户可能大体是透明的。根据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间解析和分割数据。下面讨论其中集成了安全数据解析器的系统的某些说明性例子。

[0476] 本发明的安全数据解析器可被集成到操作系统内核中（例如，Linux，Unix或其他适合的商业或专用操作系统）。这种集成可用于在设备级保护数据，从而例如通常存储在一个或多个设备内的数据被集成到操作系统内的安全数据解析器划分为某个数目的部分，并且被存储在一个或多个设备间。当试图访问原始数据时，同样被集成到操作系统内的适当软件可以用可能对端用户透明的方式将解析的数据部分重组为原始数据。

[0477] 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意其他适合的组件内，以便跨任意或所有支持的平台保护本地和联网的数据存储。例如，采用集成的安全数据解析器，存储系统可以使用由安全数据解析器提供的冗余（即，该冗余用于实现需要比数据的全部分离部分少的部分以便重构原始数据的特征）以便防止数据丢失。安全数据解析器还允许写入存储设备的所有数据，不论是否使用冗余，处于根据本发明的解析产生的多个部分的形式。当试图访问原始数据时，同样集成到卷管理器或存储系统的其他适当组件内的适当软件可以用对端用户可能为透明的方式将解析的数据部分重组为原始数据。

[0478] 在一种适合的方法中，本发明的安全数据解析器可被集成到RAID控制器内（作为硬件或软件）。这允许数据到多个驱动器的安全存储，同时在驱动器故障的情况下保持容错性。

[0479] 本发明的安全数据解析器可被集成到数据库内，以便例如保护敏感表格信息。例如，在一种适合的方法中，可以根据本发明解析和划分（例如，不同部分被存储在位于一个或多个位置的一个或多个存储设备上或单个存储设备上）与数据库表的特定单元相关联的数据（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）。可以按传统的验证方法批准访问重组部分以便观看原始数据（例如，用户名和口令询问）。

[0480] 本发明的安全数据解析器可被集成到涉及运动中数据的任意适当系统内（即，数据从一个位置到另一个位置的传输）。这种系统包括，例如，电子邮件，流数据广播，以及无线（例如 WiFi）通信。对于电子邮件，在一个适合的方法中，安全解析器可用于解析外出消息（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）），并且沿不同路径发送解析的数据的不同部分，从而创建多个数据流。如果这些数据流中的任意一个受到危及，由于根据本发明系统可能需要组合多于一个部分以便产生原始数据，原始消息保持安全。在另一个适当的方法中，可以沿着一个路径顺序地传输不同数据部分，从而如果获得了一个部分，其不足以产生原始数据。不同部分到达预期接收方的位置，并且可被根据本发明组合以便产生原始数据。

[0481] 图 28 和 29 是这种电子邮件系统的说明性方框图。图 28 示出了发送方系统 2700，其可以包括任意适合的硬件，诸如计算机终端，个人计算机，手持设备（例如，PDA，黑莓），蜂窝电话，计算机网络，任意适合的硬件，或其任意组合。发送方系统 2700 用于产生和 / 或存储消息 2704，消息 2704 可以是例如电子邮件消息，二进制数据文件（例如，图形，语音，视频等）或这两者。安全数据解析器 2702 根据本发明解析和分割消息 2704。可以在网络 2708 上（例如，Internet，内联网，LAN，WiFi，蓝牙，任意其他适合的硬布线或无线通信装置，或其任意组合）通过一个或多个分离的通信路径 2706 将结果数据部分传递到接收方系统 2710。数据部分可被在时间上并行地传递，或可替换地，根据不同数据部分的传递之间的任意适合的时间延迟传递。如上面关于发送方 2700 所描述的，接收方系统 2710 可以是任意适合的硬件。根据本发明在接收方系统 2710 重组在通信路径 2706 上传送的分离的数据部分，以便产生原始消息或数据。

[0482] 图 29 示出了发送方系统 2800，其可以包括任意适合的硬件，诸如计算机终端，个人计算机，手持设备（例如，PDA），蜂窝电话，计算机网络，任意适合的硬件，或其任意组合。发送方系统 2800 用于产生和 / 或存储消息 2804，消息 2804 可以是例如电子邮件消息，二进制数据文件（例如，图形，语音，视频等）或这两者。安全数据解析器 2802 根据本发明解析和分割消息 2804。可以在网络 2808 上（例如，Internet，内联网，LAN，WiFi，蓝牙，任意其他适合的通信装置，或其任意组合）通过单个通信路径 2806 将结果数据部分传递到接收方系统 2810。可以在通信路径 2806 上相对于彼此串行地传递数据部分。如上面关于发送方 2800 所描述的，接收方系统 2810 可以是任意适合的硬件。根据本发明在接收方系统 2810 处重组在通信路径 2806 上传送的分离的数据部分，以便产生原始消息或数据。

[0483] 应当理解，图 28 和 29 的布置仅是说明性的。可以使用任意其他适合的布置。例如，在另一个适合的方法中，可以组合图 28 和 29 的系统的特征，从而使用图 28 的多路径方法，并且其中通信路径 2706 中的一个或多个如图 29 的上下文中的通信路径 2806 那样用于传递多于一个的数据部分。

[0484] 安全数据解析器可被集成到运动中数据(data-in motion)系统的任意适合级别。例如,在电子邮件系统的上下文中,安全解析器可被集成到用户接口层(例如,集成到Microsoft® Outlook),在该情况下,用户在使用电子邮件时可以控制对安全数据解析器特征的使用。可替换地,安全数据解析器可被集成到后端组件诸如在交换服务器,在该情况下,可以根据本发明自动解析、分割和沿不同路径传递消息而不需要任何用户干涉。

[0485] 类似地,在数据流广播的情况下(例如,音频,视频),可将外出的数据解析和分割为多个流,每个流包含解析的数据的一部分。可以沿着一个或多个路径传递多个流,并且根据本发明在接收方的位置进行重组。这种方法的一个益处是其避免了相对大的与传统数据加密并且接着在单个通信通道上传输加密的数据相关联的开销。本发明的安全解析器允许在多个并行流发送运动中数据,这增加了速度和效率。

[0486] 应当理解,可以集成安全数据解析器以便保护和容错通过任意传输介质的任意类型的运动中数据,包括例如,有线,无线或物理的传输介质。例如,Internet 上的语音协议(VoIP)应用可以使用本发明的安全数据解析器。可以使用本发明的安全数据解析器保护来自或到诸如黑莓和智能电话的任意适合的个人数字助理(PDA)设备的有线或无线数据传输。使用用于点到点和基于集线器的无线网络的无线 802.11 协议的通信、卫星通信、点到点无线线通信、Internet 客户机/服务器通信或任意其他适合的通信可以涉及根据本发明的安全数据解析器的运动中数据的能力。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,生物测定验证设备(例如,指纹扫描器)或任意其他适合的外围设备)之间的,计算机与计算机外围设备之间的,计算机外围设备和任意其他适合的设备之间的数据通信或其任意组合可以使用本发明的运动中数据特征。

[0487] 使用例如分离的路线、交通工具、方法、任意其他适合的物理运输或其任意组合,本发明的运动中数据特征还可应用于安全份的物理运输。例如,数据的物理运输可以发生在数字/磁带,软盘,光盘,物理标记,USB 驱动器,可移动硬件驱动器,具有闪存的消费电子设备(例如,Apple IPOD 或其他 MP3 播放器),闪存,用于传输数据的任意其他适合的介质或其任意组合上。

[0488] 本发明的安全数据解析器可以提供具有灾难恢复能力的安全性。根据本发明,可不必须需要由安全数据解析器产生的分离数据的所有部分就可以取回原始数据。即,在存储的 m 个部分中,需要这些 m 个部分中的最少 n 个数目以便取回原始数据,其中 n ＜＝ m。例如,如果 4 个部分中的每一个相对于其他 3 个部分存储在不同的物理位置,则如果在这个例子中 n ＝ 2,这些位置中的两个可能受到了危及从而数据被毁坏或不可访问,可能仍可以从另外两个位置的部分中取回原始数据。可以使用任意适合的 n,m 值。

[0489] 另外,本发明的 m 个特征中的 n 个可用于创建“两人规则”,以便防止将对可能是敏感数据的内容的完整访问权委托给单个个体或任意其他实体,每个具有以本发明的安全解析器解析的划分数据的一部分的一个或两个不同的实体可能需要同意将它们的部分放置在一起,以便取回原始数据。

[0490] 本发明的安全数据解析器可用于给一组实体提供组范围密钥,组范围密钥允许组成员访问由特定组授权访问的特定信息。组密钥可以是根据本发明的安全解析器产生的数据部分之一,可能需要它以便与集中存储的另一部分组合例如以检索寻找的信息。该特征允许例如组中的安全合作。它可被应用于例如专用网络,虚拟私有网络,内联网,或任意其

他适合的网络。

[0491] 安全解析器的这种用途的特定应用包括例如联合信息共享，其中例如给予多个国际友好政府军队在授权给各个国家的安全级别上在单个网络或对偶网络（即，与当前使用的涉及相对基本上手工处理的许多网络相比）传递运算和其他敏感数据的能力。这种能力还适用于公司或其他组织，其中可以在单个网络上传递一个或多个特定个体（组织内或之外）需要知道的信息，而不需担心未授权的个体观看该信息。

[0492] 另一个特定应用包括政府系统的多级安全层次。即，本发明的安全解析器可以提供使用单个网络以不同分类信息级别（例如，未分类，分类的，秘密，机密）运转政府系统的能力。如果希望，可以使用多个网络（例如，用于机密的单独网络），但是本发明允许比当前为每个分类级别使用单独网络少得多的布置。

[0493] 可以使用本发明的安全解析器的上述应用的任意组合。例如，组密钥应用可与运动中数据安全应用一起使用（即，在网络上传递的数据仅能被相应组的成员访问，并且当数据处于运动中时，它被根据本发明分割到多个路径中（或以顺序部分发送））。

[0494] 本发明的安全数据解析器可被集成到任意中间件应用，以便使得应用能够安全地将数据存储到不同数据库产品，或存储到不同设备而不用修改应用或数据库。中间件是用于允许两个单独并且已存在的程序通信的任意产品的术语。例如，在一个适合的方法中，可以使用集成了安全数据解析器的中间件，以便允许为特定数据库编写的程序与没有定制编码的其他数据库通信。

[0495] 可以实现具有任意适合功能（诸如此处讨论的那些）的任意组合的本发明的安全数据解析器。在本发明的某些实施例中，例如，可以实现仅具有某些功能的安全数据解析器，而可以通过使用直接或间接与安全数据解析器接口的外部软件，硬件或这两者获得其他功能。

[0496] 例如图 30 以安全数据解析器 3000 示出了安全数据解析器的说明性实现。安全数据解析器 3000 可被实现为具有非常少的内置功能。如所示出的，安全数据解析器 3000 可以包括用于根据本发明使用模块 3002 将数据解析和分割为数据部分（此处还称为份）的内置功能。安全数据解析器 3000 还可以包括用于使用模块 3004 执行冗余，以便能够实现例如上述 m of n 特征的内置功能（即，使用少于全部解析和分割的数据创建原始数据）。安全数据解析器 3000 还可以包括份分配功能，其使用模块 3006 以便根据本发明将数据份放置在缓冲区内，从缓冲区发送数据份，以便传递到远程位置进行存储等。应当理解，任意其他适合的功能可被内置在安全数据解析器 3000 内。

[0497] 组装数据缓冲区 3008 可以是用于存储将被安全数据解析器 3000 解析和分割的原始数据（虽然不必处于其原始形式）的任意适合的存储器。在分割操作中，组装数据缓冲区 3008 给安全数据解析器 3008 提供输入。在恢复操作中，组装数据缓冲区 3008 用于存储安全数据解析器 3000 的输出。

[0498] 分割份缓冲区 3010 可以是一个或多个存储器模块，其可用于存储通过解析和分割原始数据而获得的数据的多个份。在分割操作中，分割份缓冲区 3010 保持安全数据解析器的输出。在恢复操作中，分割份缓冲区保持安全数据解析器 3000 的输入。

[0499] 应当理解，安全数据解析器 3000 中可以内置任意其他适合的布置。可以内置任意附加的特征，并且可以去除任意示出的特征，使其更可靠，减少可靠性，或以任意适合的方

式进行修改。缓冲区 3008 和 3010 仅是说明性的，并且可被以任意适合的方式修改，删除，或添加。

[0500] 以软件，硬件或这两者实现的任意适合的模块可被称为或称作安全数据解析器 3000。如果希望，甚至可以用一个或多个外部模块取代内置于安全数据解析器 3000 的功能。如所示出的，某些外部模块包括随机数产生器 3012，密码反馈密钥产生器 3014，散列算法 3016，任意一种或几种加密 3018，以及密钥管理 3020。应当理解这些仅是说明性的外部模块。除了所示模块之外或取代所示模块，可以使用任意其他适合的模块。

[0501] 密码反馈密钥产生器 3014 可以在安全数据解析器 3000 外部地为每个安全数据解析器操作产生唯一密钥或随机数（使用例如随机数产生器 3012），该密钥或随机数被用作将原始会话密钥大小扩展到等于将被解析和划分的数据的长度的值（例如，128，256，512 或 1024 位的值）的操作的种子值。任意适合算法可被用于密码反馈密钥产生，包括例如，AES 密码反馈密钥产生算法。

[0502] 为了便于将安全数据解析器 3000 和其外部模块（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），可以使用例如可以使用 API 函数的包装层。可以使用便于将安全数据解析器层 3026 集成到应用层 3024 中的任意其他适合的布置。

[0503] 图 31 说明性地示出了当应用层 3024 中发出了写（例如，写到存储设备），插入（例如，插入数据库字段内），或传输（例如，在网络上传输）命令时，可以如何使用图 30 的布置。在步骤 3100，识别将被保护的数据，并且调用安全数据解析器。在步骤 3102 通过掩饰器层 3022 传递该调用，掩饰器层 3022 将在步骤 3100 识别的输入数据流传输到组装数据缓冲区 3008。在步骤 3102，还存储任意适合的份信息，文件名，任意其他适合的信息或其任意组合（例如，作为掩饰器层 3022 处的信息 3106）。安全数据处理器 3000 然后根据本发明解析和分割从组装数据缓冲区 3008 作为输入获得的数据。它将数据份输出到分割的份缓冲区 3010。在步骤 3104，掩饰器层 3022 从存储的信息 3106 中获得任意适合的份信息（即，由掩饰器 3022 在步骤 3102 存储的）和份位置（多个）（例如，从一个或多个配置文件）。掩饰器层 3022 然后适当地（例如，写到一个或多个连接到网络上的存储设备等）写输出份（从分割的份缓冲区 3010 获得的）。

[0504] 图 32 说明性地示出了当发生读（例如，从存储设备读），选择（例如，当从数据库字段中选择），或接收（例如，从网络接收）时，如何使用图 30 的布置。在步骤 3200，识别将要恢复的数据，并且从应用层 3024 调用安全数据解析器 3000。在步骤 3202，从掩饰器层 3022 获得任意适合的份信息并且确定份位置。掩饰器层 3022 将在步骤 3200 识别出的数据部分装入分割的份缓冲区 3010。然后安全数据解析器 3000 根据本发明处理这些份（例如，如果仅可获得 4 份中的 3 份，可以使用安全数据解析器 3000 的冗余功能仅使用这 3 份恢复原始数据）。然后将恢复的数据存储到组装数据缓冲区 3008。在步骤 3204，应用层 3022 将存储在组装数据缓冲区 3008 内的数据转换为其原始数据格式（如果需要），并且将原始格式的原始数据提供给应用层 3024。

[0505] 应当理解，图 31 所示的解析和分割原始数据和图 32 所示的将数据部分恢复为原始数据仅是说明性的。除了所示这些之外或取代所示这些，可以使用任意其他适合的处理、组件或这两者。

[0506] 图 33 是根据本发明的一个实施例用于将原始数据解析和分割为两个或多个数据部分的说明性处理流的方框图。如所示出的，将被解析和分割的原始数据为纯文本 3306（即，作为例子使用的单词“SUMMIT”）。应当理解，根据本发明可以解析和分割任意其他类型的数据。产生会话密钥 3300。如果会话密钥 3300 的长度与原始数据 3306 的长度不兼容，可以产生密码反馈会话密钥 3304。

[0507] 在一个适合的方法中，在解析，分割或这两者之前可以加密原始数据 3306。例如，如图 33 所示，可将原始数据 3306 和任意适合的值异或（例如与密码反馈会话密钥 3304，或与任意适合的值）。应当理解，取代或除了异或技术之外，可以使用任意其他适合的加密技术。还应当理解，虽然图 33 以按字节的操作进行了说明，操作可以发生在位级或任意其他适合的级别。还应当理解，如果希望，不需要原始数据 3306 的任何加密。

[0508] 对得到的加密数据（或如果不发生加密，原始数据）进行散列，以便确定如何在输出桶之间（例如，在示出的例子中 4 个之间）分割加密（原始）数据。在示出的例子中，散列以字节进行并且是密码反馈会话密钥 3304 的函数。应当理解，这仅是说明。如果希望，可以在位级别执行散列。散列可以是除了密码反馈会话密钥 3304 之外的任意其他适合的值的函数。在另一个适合的方法中，不需要散列。而是可以采用用于分割数据的任意其他适合的方法。

[0509] 图 34 是根据本发明的一个实施例，用于从原始数据 3306 的两个或多个解析和分割部分中恢复原始数据 3306 的说明性处理流的方框图。该处理涉及以密码反馈会话密钥 3304 的函数相反地散列所述部分（即与图 33 的处理相反），以便恢复加密的原始数据（或如果在解析和分割之前没有加密，原始数据）。加密密钥然后被用于恢复原始数据（即，在示出的例子中，通过将其与加密数据异或，密码反馈会话密钥 3304 用于解密异或加密）。这恢复原始数据 3306。

[0510] 图 35 示出了在图 33 和 34 的例子中可以如何实现位分割。可以使用散列（例如，作为密码反馈会话密钥的函数，作为任意其他适合值的函数），以便确定分割数据的每个字节的位值。应当理解，这仅是实现在位级别分割的一个说明性方法。可以使用任意其他适合的技术。

[0511] 应当理解，此处对散列功能的任意提及可以相对于任意适合的散列算法进行。这包括例如 MD5 和 SHA-1。可以在不同时间并且由本发明的不同组件使用不同的散列算法。

[0512] 在根据上面说明性的程序或通过任意其他过程或算法确定了分割点之后，可以做出关于将左段和右段中的每一个附加到哪些数据部分的确定。可以使用用于做出这个确定的任意适合的算法。例如，在一个适合的方法中，可以创建所有可能的分配的表（例如，以左段的目的地和右段的目的地的对的形式），从而可以通过使用会话密钥、密码反馈会话密钥、或可能产生并且延长到原始数据大小的任意其他适合的随机或伪随机值中的相应数据的任意适合的散列函数，确定左段和右段中的每一个的目的地份值。例如，可以使用随机或伪随机值值的相应字节的散列函数。使用该散列函数的输出确定从所有目的地组合的表中选择哪个目的地对（即，用于左段的一个和用于右段的一个）。基于这个结果，将分割的数据单元的每个段附加到按照散列函数的结果选择的表值所指出的相应的两个份。

[0513] 根据本发明可以在数据部分上附加冗余信息，以便允许使用少于全部数据部分恢复原始数据。例如如果希望 4 个部分中的 2 个部分足以恢复数据，则可以以例如轮流方式

将来自这些份的附加数据相应地附加到每个份（例如，在原始数据的大小为 4MB 时，份 1 获得其自身的份以及份 2 和 3 的份；份 2 获得其自身的份以及份 3 和 4 的份；份 3 获得其自身的份以及份 4 和 1 的份；并且份 4 获得其自身的份以及份 1 和 2 的份）。根据本发明可以使用任意这种适合的冗余。

[0514] 应当理解，根据本发明可以使用任意其他适合的解析和分割方法，以便从原始数据集产生数据部分。例如，可以基于位随机或伪随机地处理解析和分割。可以使用随机或伪随机值（例如，会话密钥、密码反馈会话密钥等），从而对于原始数据值的每个位，关于随机或伪随机值中的相应数据的散列函数的结果可以指示将相应位附加到哪个份。在一个适合的方法中，随机或伪随机值可被产生为或延长到原始数据大小的 8 倍，从而可以相对于原始数据的每个位，对随机或伪随机值的相应字节执行散列函数。根据本发明可以使用在位级别解析和分割数据的任意其他适合的算法。还应当理解，根据本发明可以，诸如例如，以上面刚刚描述的方式将冗余数据附加到数据份。

[0515] 在一个适合的方法中，解析和分割不需要是随机或伪随机的。而是可以使用用于解析和分割数据的任意适合的确定性算法。例如，可以采用将原始数据分解为连续的份作为解析和分割算法。另一个例子是按位解析和分割原始数据，以轮流方式将每个相应的位顺序地附加到数据份。还应当理解，根据本发明可以用例如上述方式将冗余数据添加到数据份。

[0516] 在本发明的一个实施例中，在安全数据解析器产生原始数据的若干部分之后，为了恢复原始数据，某个或多个产生的部分可以是强制性的。例如，如果这些部分之一用作验证份（例如，保存在物理标记设备上），并且如果使用安全数据解析器的容错特征（即，需要少于全部部分以恢复原始数据），则即使安全数据解析器可以访问原始数据的足够数目的部分以恢复原始数据，在恢复原始数据之前可能需要存储在物理标记设备上的验证份。应当理解，基于例如应用，数据类型，用户，任意其他适合的因素或其任意组合，可能需要任意数目和类型的特定份。

[0517] 在一个适合的方法中，安全数据解析器或安全数据解析器的某些外部组件可以加密原始数据的一个或多个部分。可能需要提供加密部分并且对其解密以便恢复原始数据。可以用不同的加密密钥加密不同的加密部分。例如，这个特征可用于实现更安全的“双人规则”，从而第一个用户必须具有使用第一加密加密的特定份，并且第二个用户必须具有使用第二加密密钥加密的特定份。为了访问原始数据，两个用户需要具有其各自的加密密钥，并且提供其原始数据的相应部分。在一个适合的方法中，可以使用公钥加密一个或多个数据部分，这些部分可以是恢复原始数据所需的强制份。然后可以使用私钥解密该份，以便用于恢复原始数据。

[0518] 在需要少于所有份以恢复原始数据的情况下，可以使用利用强制份的任意这种适合的范例。

[0519] 在本发明的一个适合的实施例中，可以随机或伪随机地处理将数据分配到有限数目的数据份，从而从统计的角度看，数据的任意特定份接收数据的特定单元的概率等于剩余份中的任意一个将接收该数据单元的概率。结果，每个数据份具有近似相等数目的数据位。

[0520] 根据本发明的另一个实施例，有限数目的数据份中的每一个不需要具有接收来自

原始数据的解析和分割的数据单元的相等概率。而是某个或更多份可以具有比其余份更高或更低的概率。结果，某些份相对于其他份可以在位大小方面更大或更小。例如，在两个份的情况下，一个份可以具有接收数据单元的1％的概率，而第二个份具有99％的概率。因此将遵从一旦安全数据解析器在两个份之间分配数据单元，第一个份应近似具有1％的数据，并且第二个份具有99％的数据。根据本发明可以使用任意适合的概率。

[0521] 应当理解还可以对安全数据解析器编程，以便根据精确的（或近似精确的）百分比将数据分配到份。例如，安全数据解析器可被编程为将80％的数据分配给第一个份，并且将剩余的20％数据分配给第二个份。

[0522] 根据本发明的另一个实施例，安全数据解析器可以产生数据份，这些份中的一个或多个具有预定的大小。例如，安全数据解析器可以将原始数据分割到数据部分，其中这些部分之一精确地为256位。在一个适合的方法中，不可能产生具有必备大小的数据部分，则安全数据解析器可以填充该部分，使其具有正确的大小。可以使用任意适合的大小。

[0523] 在一个适合的方法中，数据部分的大小可以是加密密钥，分割密钥，任意其他适合的密钥，或任意其他适合的数据元素的大小。

[0524] 如前所述，安全数据解析器可以在解析和分割数据时使用密钥。出于清楚和简洁的目的，这些密钥在此处被称为“分割密钥”。例如，前面介绍的会话主密钥是一种分割密钥。另外，如前所述，分割密钥可被保护在由安全数据解析器产生的数据的份中。可以使用用于保护分割密钥的任意适合的算法，以便在数据份中保护它们。例如，可以使用Shamir算法保护分割密钥，从而产生可用于重构分割密钥的信息，并且将其附加到数据的份上。根据本发明可以使用任意其他这种适合的算法。

[0525] 类似地，可以根据任意适合的算法诸如shamir算法在一个或多个数据份中保护任意适合的加密密钥。例如，可以使用例如shamir算法或任意其他适合的算法保护用于在解析和分割之前加密数据集的加密密钥，用于在解析和分割之后加密数据部分的加密密钥或这两者。

[0526] 根据本发明的一个实施例，通过对分割密钥、加密密钥、或任意其他适合的数据元素或其任意组合进行变换，可以使用All or Nothing Transform(AoNT)，诸如完整包变换(Full Package Transform)进一步保护数据。例如，可以根据AoNT算法对根据本发明用于在解析和分割之前加密数据集的加密密钥进行变换。然后可以例如根据Shamir算法或任意其他适合的算法将变换的加密密钥分配到数据份中。如本领域的技术人员公知的，为了重构加密密钥，必须恢复加密数据集（例如，如果根据本发明使用冗余，不需要使用全部数据份），以便访问关于根据AoNT变换的必须信息。当检索原始加密密钥时，可以使用它解密加密的数据集，以便检索原始数据集。应当理解，可以结合AoNT特征使用本发明的容错特征。即，可将冗余数据包括在数据部分中，从而需要少于全部数据部分以恢复加密的数据集。

[0527] 应当理解，取代或除了在解析和分割之前相应于数据集的相应加密密钥的加密和AoNT，可将AoNT应用于在解析和分割之后用来加密数据部分的加密密钥。类似地，可将AoNT应用于分割密钥。

[0528] 在本发明的一个实施例中，可以使用例如工作组密钥进一步加密根据本发明使用的加密密钥、分割密钥或这两者，以便给受保护的数据集提供一层额外的安全性。

[0529] 在本发明的一个实施例中，可以提供追踪何时调用了安全数据解析器以便分割数据的审查模块。

[0530] 图 36 示出了根据本发明使用安全数据解析器的组件的可能选择 3600。下面概述每个选择组合并且以图 36 中的适当步骤号标注。安全数据解析器本质上可以是模块，其允许在图 36 中示出的每个功能块内使用任意已知算法。例如，可以取代 Shamir 使用其他密钥分割（例如，秘密共享）算法诸如 Blakely，或可以用其他已知的加密算法诸如 Triple DES 取代 AES 加密。图 36 的例子中示出的标号仅示出了在本发明的一个实施例中使用的算法的一种可能组合。应当理解，取代标出的算法，可以使用任意适合的算法或算法组合。

[0531] 1)3610，3612，3614，3615，3616，3617，3618，3619

[0532] 在步骤 3610 使用以前的加密数据，该数据最终可被分割为预定的份数。如果分割算法需要密钥，可以使用在密码学上安全的伪随机数产生器，在步骤 3612 产生分割加密密钥。在被在步骤 3615 密钥分割为具有容错性的预定份数之前，在步骤 3614 可以可选择地使用 All or Nothing Transform(AoTN) 将分割加密密钥变换为变换分割密钥。然后可在步骤 3616 将数据分割为预定份数。可以在步骤 3617 使用容错方案以允许以少于总份数的份数重新产生数据。一旦创建了份，可以在步骤 3618 将验证 / 完整性信息嵌入份。在步骤 3619 可以可选择地对每个份进行后加密。

[0533] 2)3111，3612，3614，3615，3616，3617，3618，3619

[0534] 在某些实施例中，可以使用由用户或外部系统提供的加密密钥加密输入数据。在步骤 3611 提供外部密钥。例如，可从外部密钥库提供密钥。如果分割算法需要密钥，可以使用在密码学上安全的伪随机数产生器，在步骤 3612 产生分割加密密钥。在被在步骤 3615 密钥分割为具有容错性的预定份数之前，可以在步骤 3614 可选择地使用 All or Nothing Transform(AoTN) 将分割密钥变换为变换分割加密密钥。然后可在步骤 3616 将数据分割为预定份数。可以在步骤 3617 使用容错方案以允许以少于总份数的份数重新产生数据。一旦创建了份，可以在步骤 3618 将验证 / 完整性信息嵌入这些份。可以在步骤 3619 可选择地对每个份进行后加密。

[0535] 3)3612，3613，3614，3615，3612，3614，3615，3616，3617，3618，3619

[0536] 在某些实施例中，可以在步骤 3612 使用在密码学上安全的伪随机数产生器产生加密密钥以便对数据进行变换。可以在步骤 3613 发生使用产生的加密密钥加密数据。可以在步骤 3614 使用 All or Nothing Transform(AoTN) 可选择地将加密密钥变换为变换加密密钥。然后在步骤 3615 将变换加密密钥和 / 或产生的加密密钥分割为具有容错性的预定份数。如果分割算法需要密钥，可以在步骤 3612 发生使用在密码学上安全的伪随机数产生器产生分割加密密钥。在被在步骤 3615 密钥分割为具有容错性的预定份数之前，可以在步骤 3614 使用 All or Nothing Transform(AoTN) 可选择地将分割密钥变换为变换分割加密密钥。然后可在步骤 3616 将数据分割为预定份数。可以在步骤 3617 使用容错方案以允许以少于总份数的份数重新产生数据。一旦创建了份，可以在步骤 3618 将验证 / 完整性信息嵌入这些份。然后可以在步骤 3619 可选择地对每个份进行后加密。

[0537] 4)3612，3614，3615，3616，3617，3618，3619

[0538] 在某些实施例中，数据可被分割为预定的份数。如果分割算法需要密钥，可以在步骤 3612 发生使用在密码学上安全的伪随机数产生器产生分割加密密钥。在步骤 3615

中密钥被分割为具有容错性的预定份数之前，可以在步骤3614使用All or Nothing Transform(AoTN)可选择地将分割密钥变换为变换分割密钥。然后可在步骤3616将数据分割。可以在步骤3617使用容错方案以允许以少于总份数的份数重新产生数据。一旦创建了份，可以在步骤3618将验证/完整性信息嵌入这些份。可以在步骤3619可选择地对每个份进行后加密。

[0539] 虽然在本发明的某些实施例中优选地使用了上面4种选择组合，在其他实施例中，可将任意其他适合的特征、步骤、或选择组合用于安全数据解析器。

[0540] 通过便于物理划分，安全数据解析器可以提供灵活的数据保护。首先可以加密数据，然后分割为具有“m of n”容错的份。当可以获得少于总份数的份数时，这允许重新产生原始信息。例如，可能丢失了某些份或在传输中破坏了某些份。如下面更详细讨论的，可以根据附加到份的容错或完整性信息重建丢失或破坏的份。

[0541] 为了创建份，安全数据解析器可选择地利用若干密钥。这些密钥可以包括下面中的一个或多个：

[0542] 预加密密钥：当选择了份预加密时，可将一个外部密钥传递给安全数据解析器。这个密钥可被外部地产生和存储在密钥库内（或其他位置），并且可用于在数据分割之前可选择地加密数据。

[0543] 分割加密密钥：可由安全数据解析器内部地产生和使用这个密钥以便在分割之前加密数据。然后可以使用密钥分割算法将这个密钥安全地存储在所述份内。

[0544] 分割会话密钥：这个密钥不用于加密算法；而是当选择了随机分割时，可用做数据划分算法的密钥。当使用随机分割时，由安全数据解析器内部地产生和使用分割会话密钥以便将数据划分为份。可以使用密钥分割算法将这个密钥安全地存储在所述份内。

[0545] 后加密密钥：当选择了份的后加密时，可将一个外部密钥传递给安全数据解析器，并且用于对各个份进行后加密。可在密钥存储器或其他适合的位置外部地产生和存储这个密钥。

[0546] 在某些实施例中，当以这种方式使用安全数据解析器保护数据时，只有给出所有所需的份和外部加密密钥，才可以重新组装信息。

[0547] 图37示出了在某些实施例中使用本发明的安全数据解析器的说明性概括处理3700。如上所述，安全数据解析器3706的两个非常适合的功能可以包括加密3702和备份3704。从而，在某些实施例中，安全数据解析器3706可被集成到RAID或备份系统或硬件或软件加密引擎。

[0548] 与安全数据解析器3706相关联的主要密钥处理可以包括预加密处理3708、加密/变换处理3710、密钥保护处理3712、解析/分配处理3714、容错处理3716、份验证处理3716和后加密处理3720中的一个或多个。如图36所示，这些处理可被以若干适合的顺序或组合执行。使用的处理组合和顺序可以取决于特定应用或用途，所需的安全级别，是否希望可选择的预加密、后加密或这两者，希望的冗余，基础或集成的系统的功能或性能，或任意其他适合的因素或因素组合。

[0549] 说明性处理3700的输出可以是两个或多个份3722。如上所述，在某些实施例中数据可被随机地（或伪随机地）分配到这些份中的每一个。在其他实施例中，可以使用确定性算法（或随机、伪随机和确定性算法的某些适合的组合）。

[0550] 除了对信息资产的单独保护之外，某些时候存在在不同用户组或利益团体中共享信息的需求。可能需要在用户组中控制对各个份的访问，或在这些用户之间共享仅允许组成员重新组装份的凭证。就此而言，在本发明的某些实施例中可将工作组密钥部署给组成员。组密钥应当受到保护并且保持机密，由于对工作组密钥的危及可能潜在地允许组外人员访问信息。下面讨论用于工作组密钥部署和保护的某些系统和方法。

[0551] 通过对存储在份中的密钥信息加密，工作组密钥概念允许对信息资产的增强保护。一旦执行了这种操作，即使暴露了所有所需的份和外部密钥，在无权使用工作组密钥的情况下，攻击者也不具重建信息的希望。

[0552] 图 38 示出了用于在份中存储密钥和数据组件的说明性方框图 3800。在图 3800 的例子中，忽略了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。

[0553] 分割数据的简化处理包括在加密阶段 3802 使用加密密钥 3804 加密数据。然后根据本发明将加密密钥 3804 的几部分分割并且存储在份 3810 内。还可以将分割加密密钥 3806 的几部分存储在份 3810 内。使用分割加密密钥，数据 3808 被分割并且存储在份 3810 内。

[0554] 为了恢复数据，可以根据本发明检索和恢复分割加密密钥 3806。然后可以逆转分割操作以恢复密文。还可以检索和恢复加密密钥 3804，并且然后使用加密密钥解密密文。

[0555] 当利用工作组密钥时，可以略微改变上述处理以便以工作组密钥保护加密密钥。可以在存储在份内之前以工作组密钥对加密密钥加密。在图 39 的说明性方框图 3900 中示出了修改的步骤。

[0556] 使用工作组密钥分割数据的简化处理包括在阶段 3902 处使用密码密钥首先加密数据。然后在阶段 3904 以工作组密钥对加密密钥进行加密。然后可将以工作组密钥加密的加密密钥分割为几部分并且与份 3912 存储在一起。还可以分割分割密钥 3908，并且将其存储在份 3912 内。最后使用分割密钥 3908 分割数据部分 3910 并且存储在份 3912 内。

[0557] 为了恢复数据，可以根据本发明检索和恢复分割密钥。然后可以根据本发明逆转分割操作以便恢复密文。可以检索和恢复加密密钥（其被以工作组密钥加密）。然后可以使用工作组密钥解密加密密钥。最后，可以使用加密密钥解密密文。

[0558] 存在用于部署和保护工作组密钥的若干保护方法。为特定应用选用哪个方法取决于若干因素。这些因素可以包括所需的安全级别，费用，方便性和工作组中用户的数目。下面提供了某些实施例中的某些常用的技术：

[0559] 基于硬件的密钥存储

[0560] 基于硬件的解决方案一般为加密系统中的加密 / 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防篡改密钥标记设备，其在便携设备（例如，智能卡 / 软件狗）或非便携密钥存储外设中存储密钥。这些设备被设计为防止未授权方容易地复制密钥材料。可由信任的机构或在硬件中产生密钥并且分配给用户。另外，许多密钥存储系统提供多因素验证，其中对密钥的使用需要访问物理对象（标记）和口令短语或生物测定两者。

[0561] 基于软件的密钥存储

[0562] 虽然基于专用硬件的存储可能是高安全性部署或应用所希望的，其他部署可以选择直接在本地硬件（例如，磁盘，RAM 或非易失 RAM 存储（器）诸如 USB 驱动器）上存储密

钥。相对于内部攻击或在攻击者能够直接访问加密机器的情况下，这提供了的较低级别的保护。

[0563] 为了在磁盘上保护密钥，基于软件的密钥管理通常通过借助根据其他验证度量的组合导出的密钥，以加密形式存储密钥以保护密钥，所述验证度量包括：口令和口令短语，给出其他密钥（例如，来自基于硬件的解决方案），生物测定或上述任意适合的组合。由这种技术提供的安全级别的范围可以从由某些操作系统（例如，MS Windows 和 Linux）提供的相对弱的密钥保护机制到使用多因素验证实现的更可靠的解决方案。

[0564] 可以有利地在若干应用和技术中使用本发明的安全数据解析器。例如，电子邮件系统，RAID 系统，视频广播系统，数据库系统，带备份系统，或任意其他适合的系统可以在任意适合的级别集成安全数据解析器。如前所述，应当理解还可以为了任意传输介质上的任意类型的运动中数据的保护和容错集成安全数据解析器，包括例如，有线、无线、或物理传输介质。作为一个例子，网际协议上的语音 (VoIP) 应用可以使用本发明的安全数据解析器解决关于 VoIP 中常见的回声和延迟的问题。通过使用即使在丢失预定数目的份的情况下也可保证包传递的容错，可以消除对关于丢包的网络重试的需要。还可以用最小的延迟和缓冲“在飞行中”有效地分割和恢复数据包（例如，网络包），产生用于各种运动中数据的全面的解决方案。安全数据解析器可以作用于网络数据包、网络语音包、文件数据块，或任意其他适合的信息单元。除了与 VoIP 应用集成之外，安全数据解析器可被与文件共享应用（例如，点到点文件共享应用），视频广播应用，电子表决或投票应用（其可以实现电子表决协议和盲签名，诸如 Sensus 协议），电子邮件应用，或可能需要或希望安全通信的任意其他网络应用集成在一起。

[0565] 在某些实施例中，可由本发明的安全数据解析器在两个不同阶段提供对运动中的网络数据的支持 - 包头产生阶段和数据划分阶段。图 40A 和 40B 分别示出了简化的包头产生处理 4000 和简化的数据划分处理 4010。可以对网络包，文件系统块，或任意其他适合的信息执行这些处理中的一个或两者。

[0566] 在某些实施例中，可以在发起网络数据包流时执行一次包头产生处理 4000。在步骤 4002，可以产生随机（或伪随机）分割加密密钥 K。然后可以在 AES 密钥掩饰步骤 4004 可选择地加密（例如使用上述工作组密钥）分割加密密钥 K。虽然在某些实施例中可以使用 AES 密钥掩饰，在其他实施例中可以使用任意适合的密钥加密或密钥掩饰算法。AES 密钥掩饰步骤 4004 可对整个分割加密密钥 K 执行，或可将分割加密密钥解析为若干块（例如，64 位的块）。然后如果希望，可以对分割加密密钥的块执行 AES 密钥掩饰步骤 4004。

[0567] 在步骤 4006，可以使用秘密共享算法（例如，Shamir）将分割加密密钥 K 分割为密钥份。然后可以将每个密钥份嵌入输出份中的一个（例如，在份包头中）。最后，可将份完整性块和（可选择地）验证后标签（例如，MAC）附加到每个份的包头块上。每个包头块可被设计为安插在单个数据包内。

[0568] 在完成包头产生之后（例如，使用简化的包头产生处理 4000），安全数据解析器可以使用简化的数据划分处理 4010 进入数据划分阶段。在步骤 4012 使用分割加密密钥 K 加密流中每个进入的数据包或数据块。在步骤 4014，可以对步骤 4012 的结果密文计算份完整性信息（例如，散列 H）。例如，可以计算 SHA-256 散列。在步骤 4016，可以根据本发明使用上述数据分割算法中的一个将数据包或数据块划分为两个或多个数据份。在某些实施例

中，可以这样分割数据包或数据块，从而每个数据份包括加密的数据包或数据块的大体随机的分配。然后将完整性信息（例如，散列 H）附加到每个数据份。在某些实施例中还可以计算可选择的验证后标签（例如，MAC），并且附加到每个数据份上。

[0569] 每个数据份可以包括元数据，这些元数据可能是允许数据块或数据包的正确重构所必需的。该信息可被包括在份的包头中。元数据可以包括这样的信息，诸如密码密钥份、密钥本体（identity），份现时（nonce），签名 /MAC 值和完整性块。为了最大化带宽效率，可以用压缩二进制格式存储元数据。

[0570] 例如，在某些实施例中，份包头可以包括明文包头信息块，其不被加密并且可以包括这样的元素，诸如 Shamir 密钥份，每个会话的现时，每个份的现时，密钥标识符（例如，工作组密钥标识符和验证后密钥标识符）。份包头还可以包括被以分割加密密钥加密的加密包头信息块。包头中还包括包括完整性包头信息块，其可以包括任意数目的以前块的完整性检查（例如，以前的两个块）。份包头中还可以包括任意其他适合的值或信息。

[0571] 如图 41 的说明性的份格式 4100 所示，包头块 4102 可以与两个或多个输出块 4104 相关联。诸如包头块 4102 的每个包头块可被设计为安插在单个网络数据包内。在某些实施例中，在包头块 4102 被从第一位置传递到第二位置之后，可以传输输出块。可替换地，可以同时并行地传输包头块 4102 和输出块 4104。传输可以发生在一个或多个类似或不类似的通信路径上。

[0572] 每个输出块可以包括数据部分 4106 和完整性 / 验证部分 4108。如上所述，可以使用包括加密的预划分数据的份完整性信息（例如 SHA-256 散列）的份完整性部分保护每个数据份。为了在恢复时检验输出块的完整性，安全数据解析器可以比较每个份的份完整性块，并且逆转分割算法。然后可以相对于份散列检验恢复的数据的散列。

[0573] 如前所述，在本发明的某些实施例中，可以结合磁带备份系统使用安全数据解析器。例如，根据本发明可将单独的磁带用作一个节点（即，部分 / 份）。可以使用任意适合的布置。例如，由两个或多个磁带组成的磁带库或子系统可被视为单个节点。

[0574] 根据本发明还可以将冗余用于磁带。例如，如果数据集被分配到四个磁带（即，部分 / 份）中，则可能需要四个磁带中的两个以便恢复原始数据。应当理解，根据本发明的冗余特征，可能需要任意适合数目的节点以便恢复原始数据。当一个或多个磁带到期时，这极大地增加了恢复的可能性。

[0575] 还可以用 SHA-256，HMAC 散列值，任意其他适合的值或其任意组合数字地保护每个磁带，以便确保防篡改。如果磁带上的数据或散列值改变，磁带将不作为恢复的候选，并且将使用剩余磁带中任意最小所需数目的磁带恢复数据。

[0576] 在常规的磁带备份系统中，当用户请求向磁带写数据或从带读数据时，磁带管理系统（TMS）给出相应于物理磁带装配的号码。这个磁带装配指向数据将被安装的物理驱动器。由人工磁带操作员或磁带库中的磁带机器人装入磁带柜。

[0577] 在本发明下，物理磁带装配可被认为是指向若干物理磁带的逻辑装配点。这不仅增加了数据容量，而且由于并行化提高了性能。

[0578] 为了增加性能，磁带节点可以是或可以包括用于存储磁带映象的 RAID 盘阵列。由于总是可以从受保护的 RAID 上获得数据，这允许高速恢复。

[0579] 虽然上面描述了安全数据解析器的某些应用，应当清楚地理解，本发明可以与任

意网络应用集成，以便增加安全性、容错、匿名或上述任意适合的组合。

[0580] 另外，鉴于此处的公开，本领域的技术人员将明了其他组合、添加、替换和修改。因此，本发明不旨在受这些优选实施例的反作用的局限，而是参考所附权利要求限定。

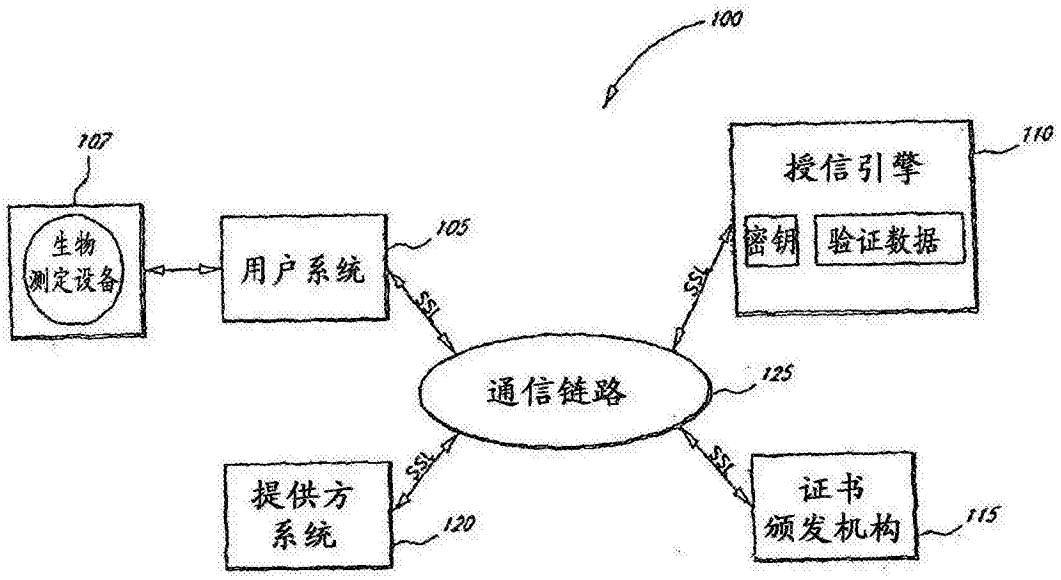

100
107
生物测定设备
用户系统
105
SSL
授信引擎
110
密钥
验证数据
通信链路
125
提供方系统
120
证书颁发机构
115

图 1

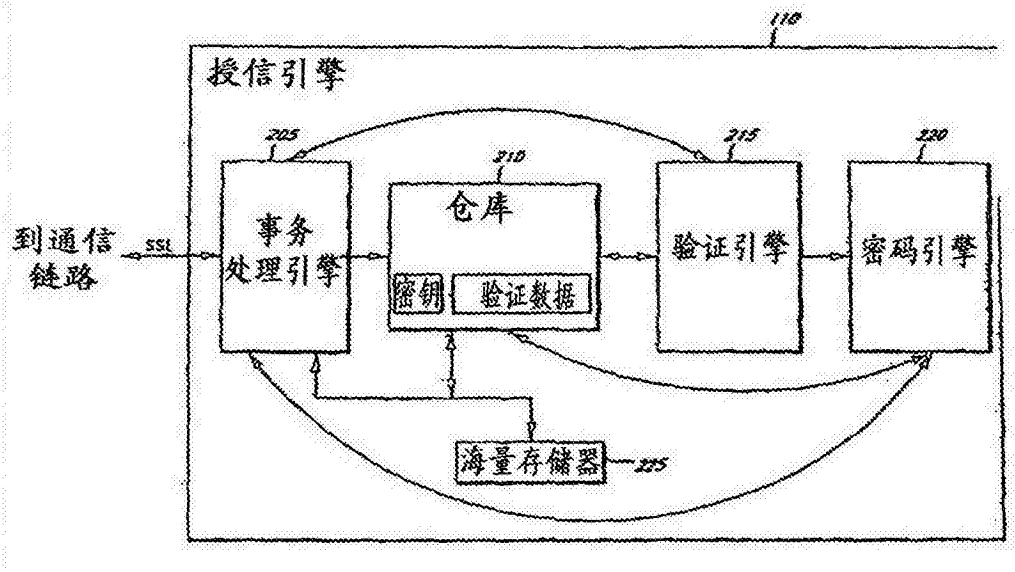

110
授信引擎
205
210
215
220
到通信链路
SSL
事务处理引擎
仓库
密钥
验证数据
验证引擎
密码引擎
海量存储器
225

图 2

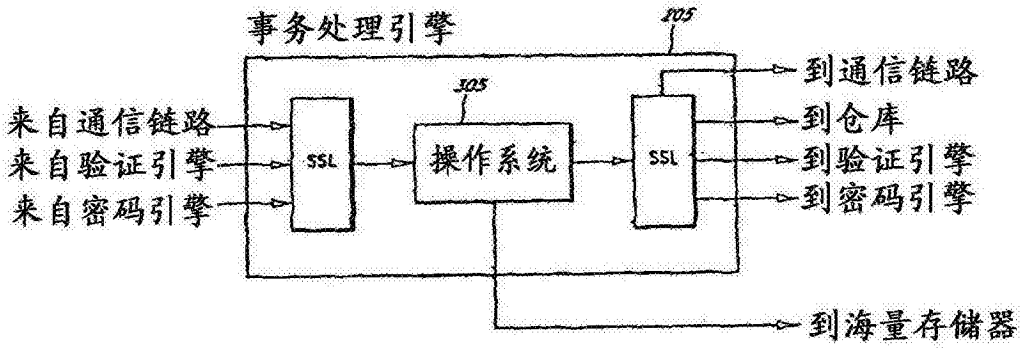

事务处理引擎
305
来自通信链路
来自验证引擎
来自密码引擎
SSL
操作系统
SSL
到通信链路
到仓库
到验证引擎
到密码引擎
到海量存储器

图 3

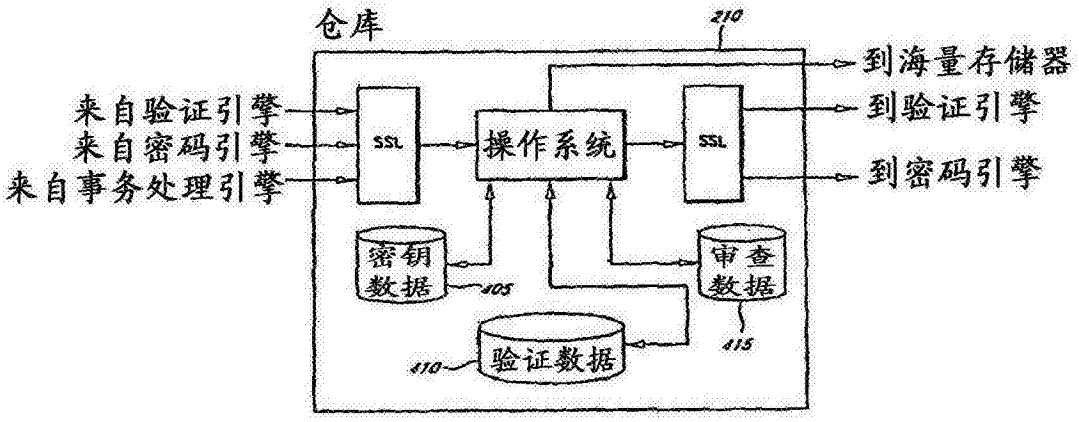

仓库
210
来自验证引擎
来自密码引擎
来自事务处理引擎
SSL
操作系统
SSL
到海量存储器
到验证引擎
到密码引擎
密钥数据
405
审查数据
415
验证数据
410

图 4

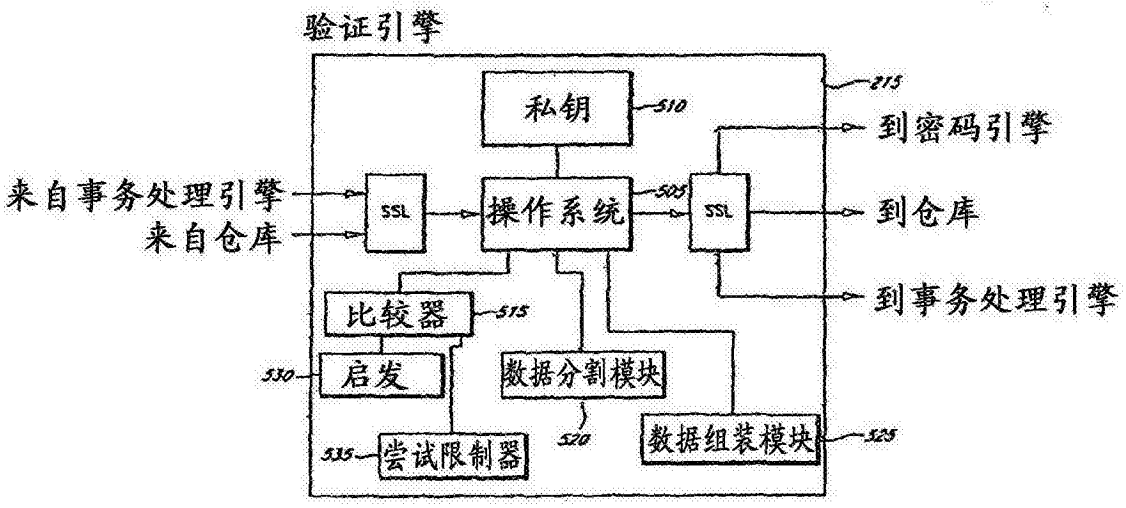

验证引擎
215
私钥
510
来自事务处理引擎
来自仓库
SSL
操作系统
505
SSL
到密码引擎
到仓库
到事务处理引擎
比较器
515
530
启发
数据分割模块
520
数据组装模块
525
535
尝试限制器

图 5

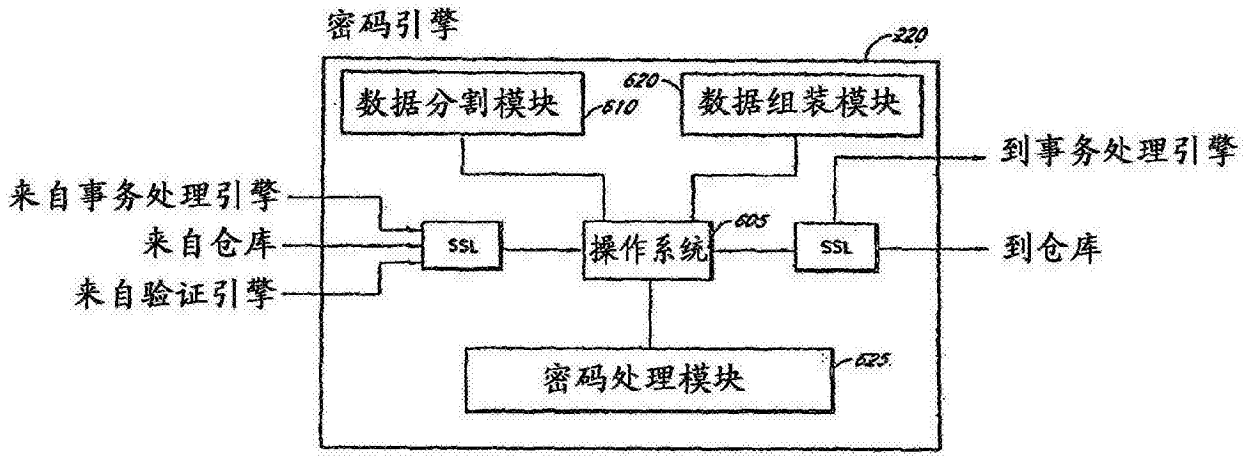

密码引擎
220
数据分割模块
610
620
数据组装模块
到事务处理引擎
来自事务处理引擎
来自仓库
来自验证引擎
SSL
操作系统
605
SSL
到仓库
密码处理模块
625

图 6

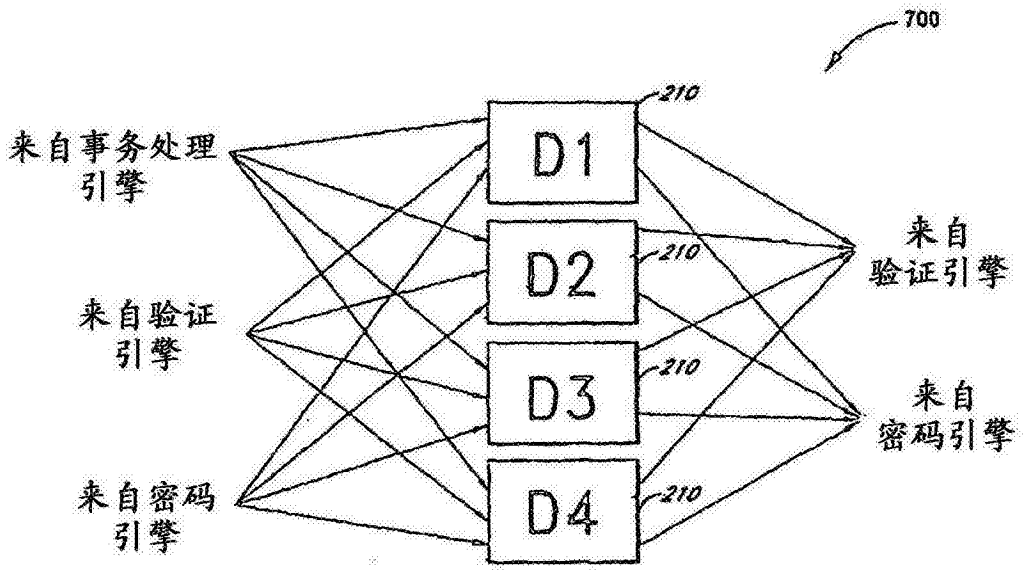

700
210
D1
D2
D3
D4
来自事务处理引擎
来自验证引擎
来自密码引擎
来自验证引擎
来自密码引擎

图 7

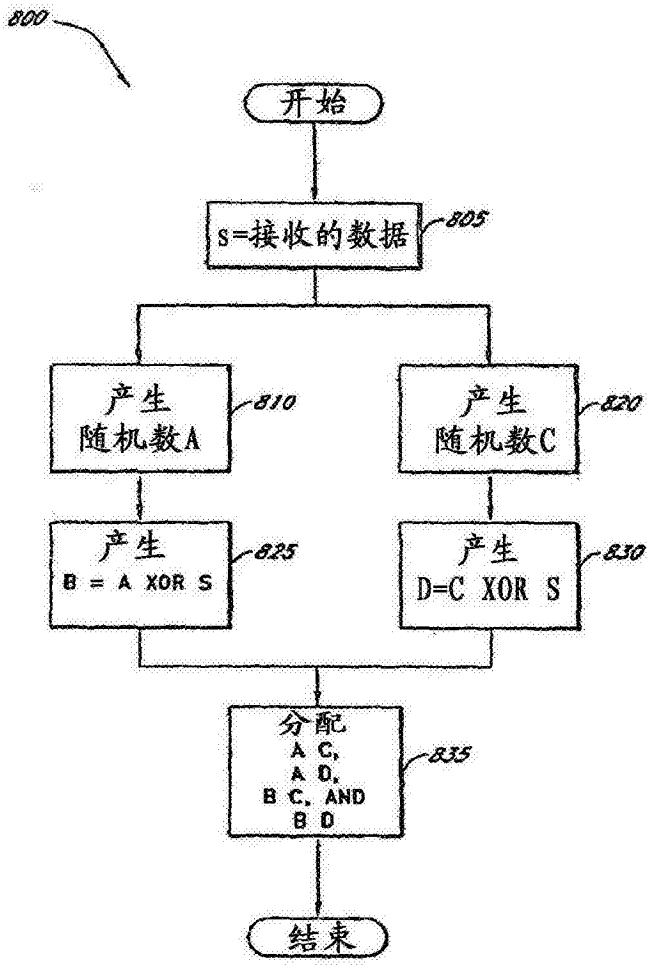

800
开始
S=接收的数据
805
产生
随机数A
810
产生
随机数C
820
产生
B = A XOR S
825
产生
D=C XOR S
830
分配
A C,
A D,
B C, AND
B D
835
结束

图 8

版面A


| 登记数据流 | | | |
|---|---|---|---|
| 发送 | 接收 | SSL | 活动 |
| 用户 | 事务处理引擎(TE) | 1/2 | 以(PUB_AE(UID, B)<br>传输登记验证数据(B)<br>和用户ID(UID)<br>以验证引擎的公钥加密(AE) |
| TE | AE | FULL | 转发传输 |
| | | | AE解密和分割转发数据 |
| AE | 第X个仓库(DX) | FULL | 存储各个数据部分 |
| 当需要数字证书时 | | | |
| AE | 密码引擎(CE) | FULL | 请求密钥产生 |
| | | | CE产生和分割密钥 |
| CE | TE | FULL | 传输对数字证书的请求 |
| TE | 证书颁发机构(CA) | 1/2 | 传输请求 |
| CA | TE | 1/2 | 传输数字证书 |
| TE | USER | 1/2 | 传输数字证书 |
| TE | MS | FULL | 存储数字证书 |
| CE | DX | FULL | 存储密钥的各个部分 |

图 9

版面B

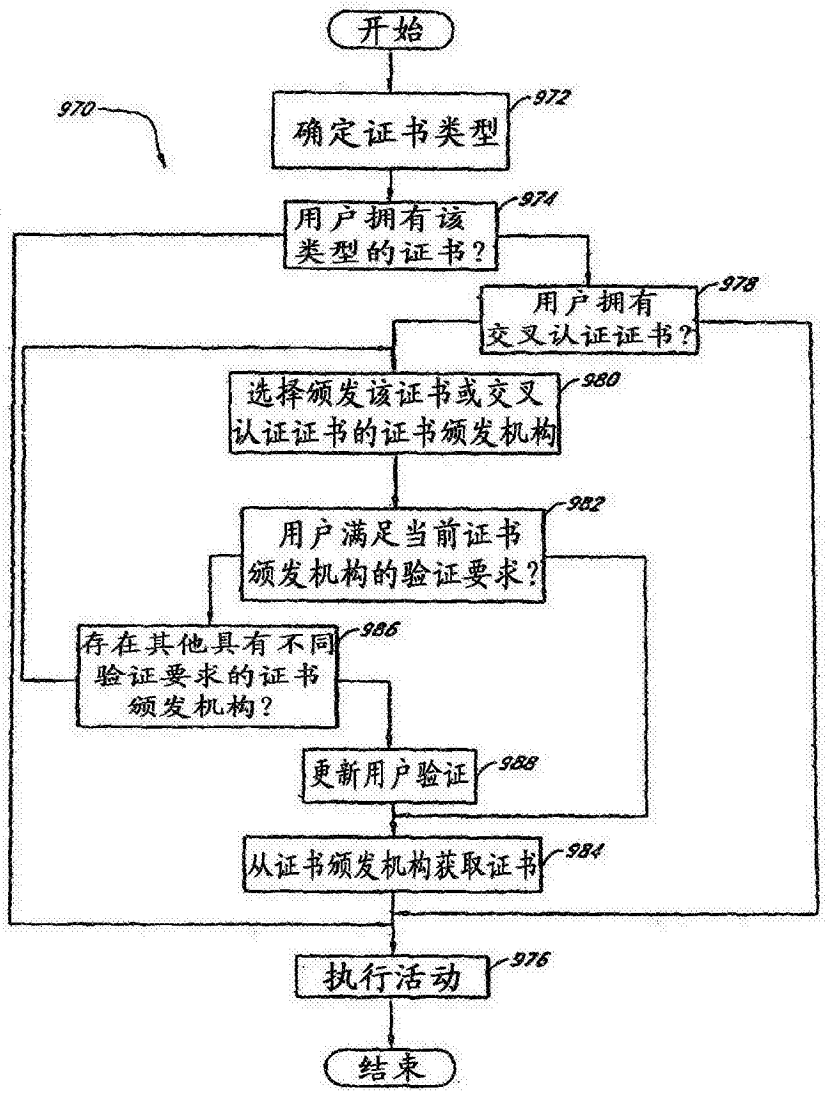

开始
970
确定证书类型
972
用户拥有该类型的证书？
974
用户拥有交叉认证证书？
978
选择颁发该证书或交叉认证证书的证书颁发机构
980
用户满足当前证书颁发机构的验证要求？
982
存在其他具有不同验证要求的证书颁发机构？
986
更新用户验证
988
从证书颁发机构获取证书
984
执行活动
976
结束

图 9


验证数据流

| | 发送 | 接收 | SSL | 活动 |
|---|---|---|---|---|
| 1005 | 用户 | 提供方 | 1/2 | 事务处理发生，诸如选择，购买 |
| 1010 | 提供方 | 用户 | 1/2 | 传输事务处理ID (TID)和验证请求(AR) |
| | | | | 从用户处产生验证数据(B′) |
| 1015 | 用户 | TE | 1/2 | 作为(PUB_AE(TID, B′))传输以验证引擎(AE)的公钥包装的TID和B′ |
| 1020 | TE | AE | 全 | 转发传输 |
| | | | | 请求和收集登记验证数据(B) |
| 1025 | 供方 | 事务处理引擎(TE) | 全 | 传输TID, AR |
| 1030 | TE | 海量存储器(MS) | 全 | 在数据块中创建记录 |
| 1035 | TE | 第X个仓库(DX) | 全 | UID, TID |
| 1040 | DX | AE | 全 | 作为(PUB_AE(TID, BX))传输TID和登记时存储的验证数据(BX) |
| 1045 | | | | |
| 1050 | | | | AE组装B和比较B′ |
| | AE | TE | 全 | AR中填写的TID |
| | TE | 提供方 | 全 | TID, 是/否 |
| 1055 | TE | 用户 | 1/2 | TID确认消息 |

图 10

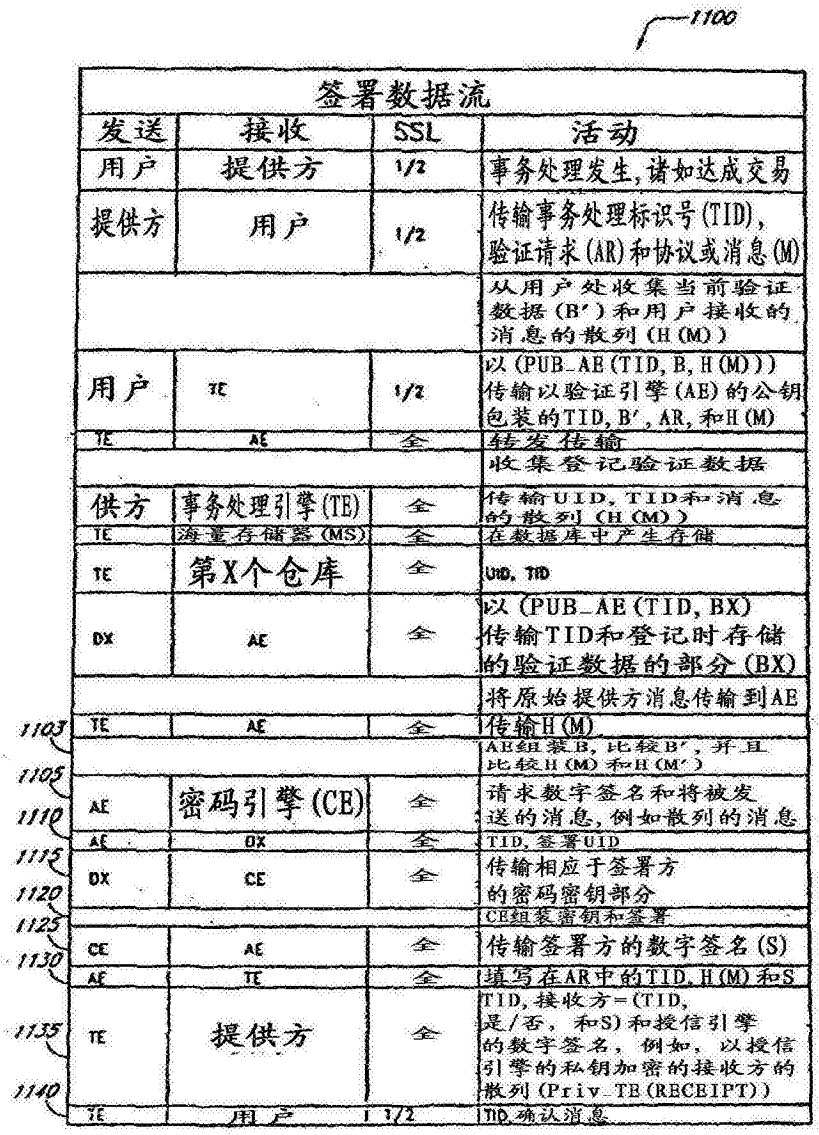

1100
签署数据流
发送 接收 SSL 活动
用户 提供方 1/2 事务处理发生,诸如达成交易
提供方 用户 1/2 传输事务处理标识号(TID),验证请求(AR)和协议或消息(M)
从用户处收集当前验证数据(B')和用户接收的消息的散列(H(M))
用户 TE 1/2 以(PUB_AE(TID,B,H(M)))传输以验证引擎(AE)的公钥包装的TID,B',AR,和H(M)
TE AE 全 转发传输
收集登记验证数据
供方 事务处理引擎(TE) 全 传输UID,TID和消息的散列(H(M))
TE 海量存储器(MS) 全 在数据库中产生存储
TE 第X个仓库 全 UID,TID
DX AE 全 以(PUB_AE(TID,BX)传输TID和登记时存储的验证数据的部分(BX)
将原始提供方消息传输到AE
1103 TE AE 全 传输H(M)
AE组装B,比较B',并且比较H(M)和H(M')
1105
1110 AE 密码引擎(CE) 全 请求数字签名和将被发送的消息,例如散列的消息
AE DX 全 TID,签署UID
1115
1120 DX CE 全 传输相应于签署方的密码密钥部分
1125 CE组装密钥和签署
1130 CE AE 全 传输签署方的数字签名(S)
AE TE 全 填写在AR中的TID,H(M)和S
1135 TE 提供方 全 TID,接收方=(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接收方的散列(Priv_TE(RECEIPT))
1140 TE 用户 1/2 TID,确认消息

图 11

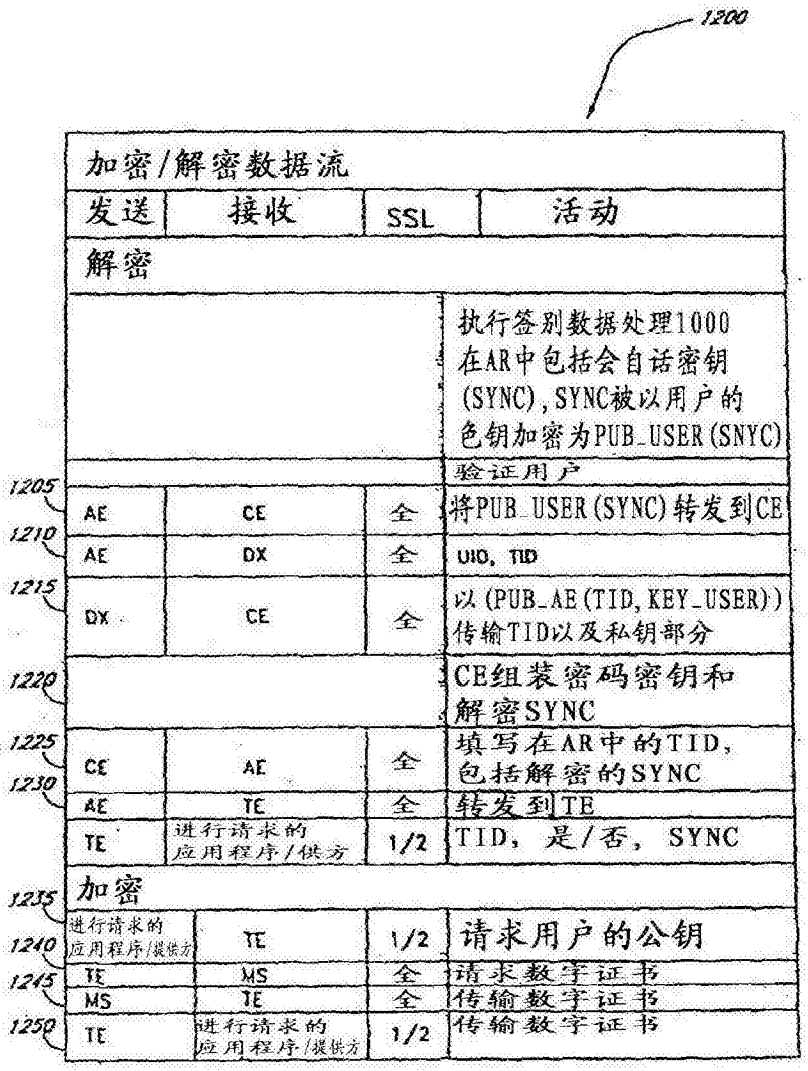

1200
加密/解密数据流
发送
接收
SSL
活动
解密
执行签别数据处理1000
在AR中包括会自话密钥
(SYNC),SYNC被以用户的
色钥加密为PUB_USER(SNYC)
验证用户
1205
AE
CE
全
将PUB_USER(SYNC)转发到CE
1210
AE
DX
全
UID, TID
1215
DX
CE
全
以(PUB_AE(TID,KEY_USER))
传输TID以及私钥部分
1220
CE组装密码密钥和
解密SYNC
1225
CE
AE
全
填写在AR中的TID,
包括解密的SYNC
1230
AE
TE
全
转发到TE
TE
进行请求的
应用程序/供方
1/2
TID, 是/否, SYNC
加密
1235
进行请求的
应用程序/提供方
TE
1/2
请求用户的公钥
1240
TE
MS
全
请求数字证书
1245
MS
TE
全
传输数字证书
1250
TE
进行请求的
应用程序/提供方
1/2
传输数字证书

图 12

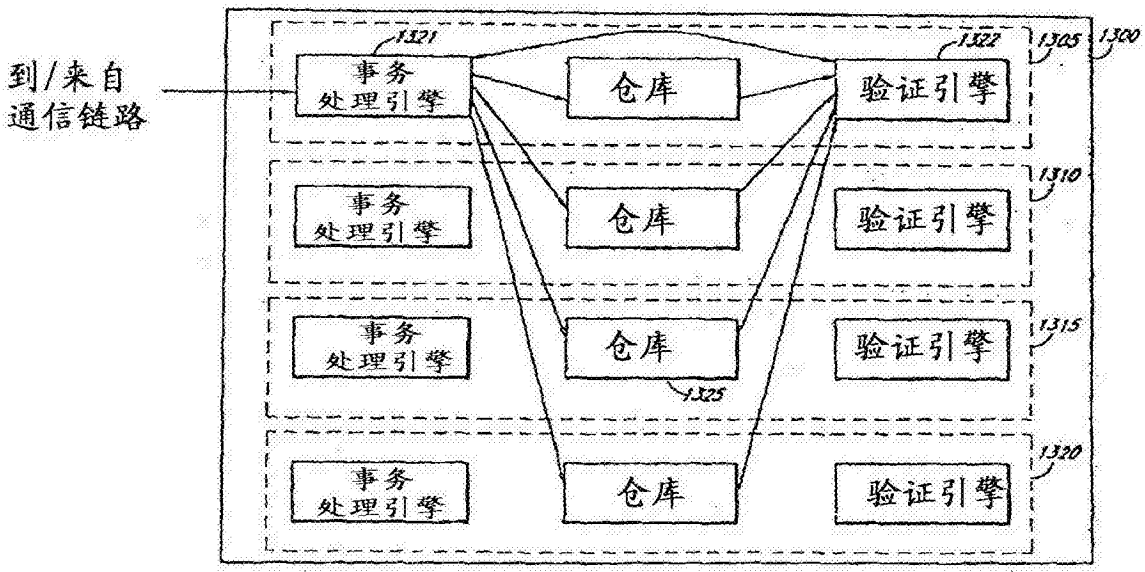

到/来自
通信链路
事务
处理引擎
仓库
验证引擎
1321
1322
1305
1300
1310
1315
1325
1320

图 13

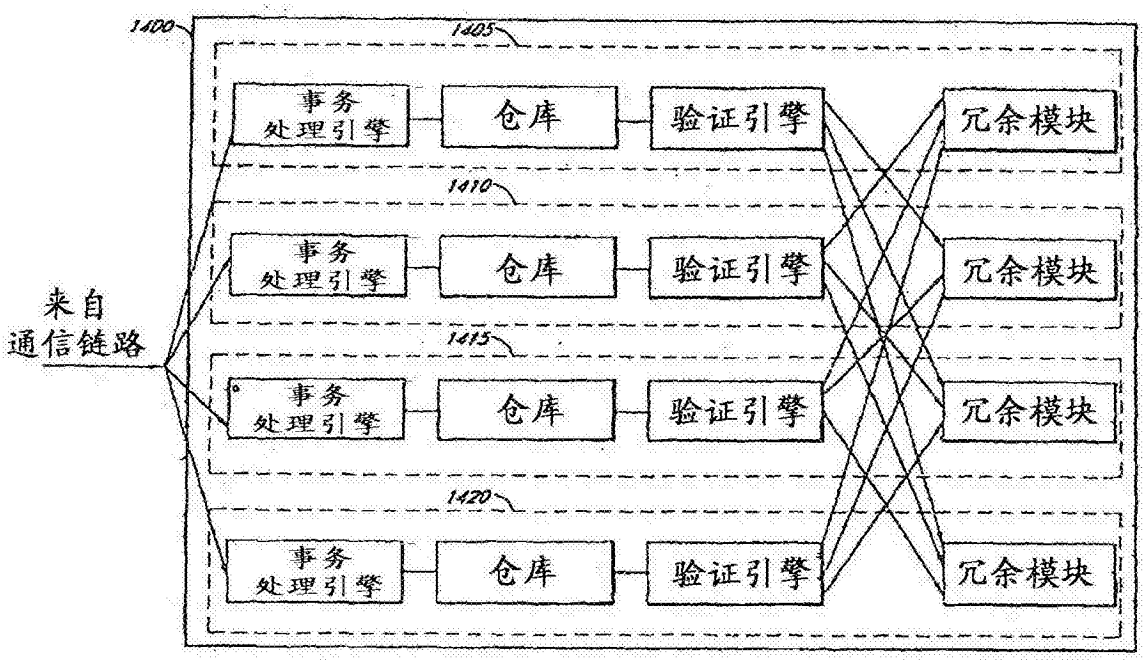

1400
1405
事务
处理引擎
仓库
验证引擎
冗余模块
1410
1415
1420
来自
通信链路

图 14

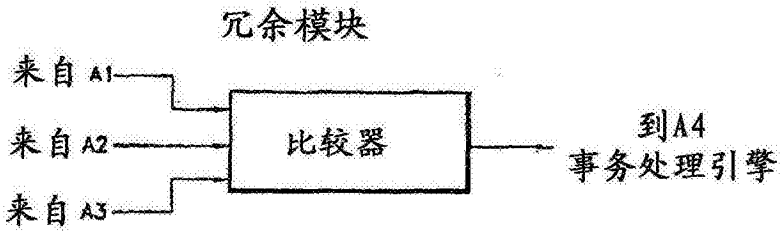

冗余模块
来自 A1
来自 A2
来自 A3
比较器
到A4
事务处理引擎

图 15

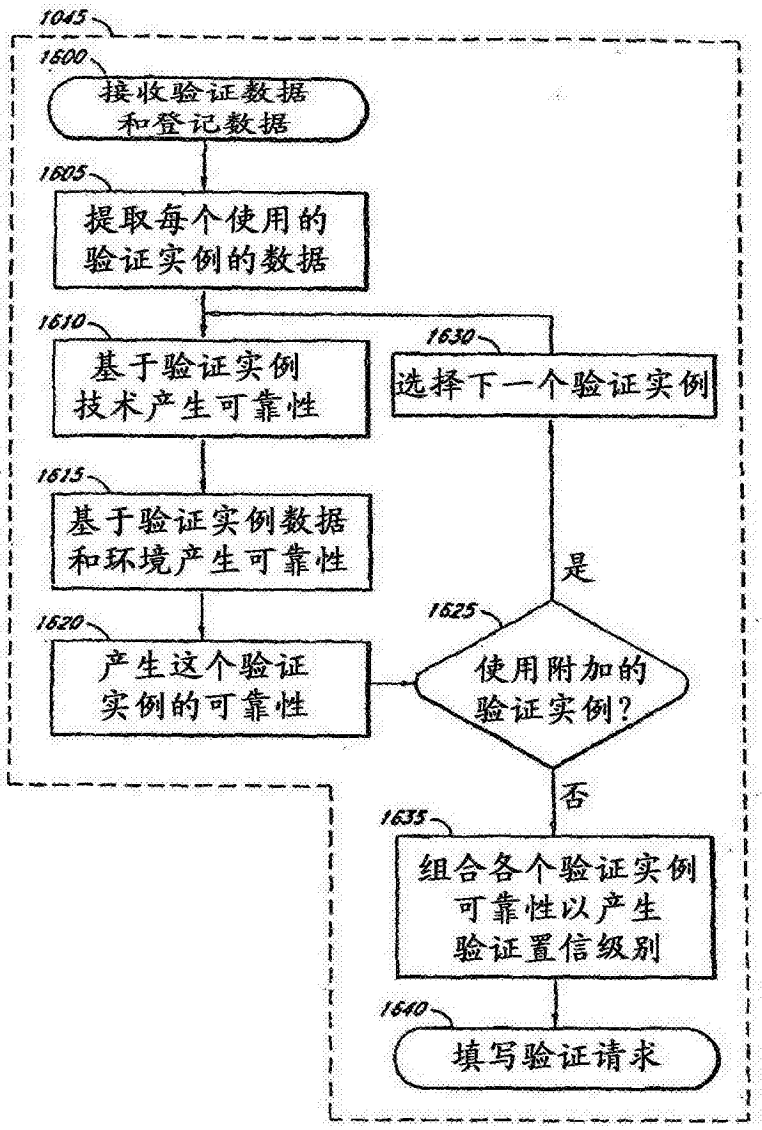

1045
1500
接收验证数据和登记数据
1605
提取每个使用的验证实例的数据
1610
基于验证实例技术产生可靠性
1615
基于验证实例数据和环境产生可靠性
1620
产生这个验证实例的可靠性
1630
选择下一个验证实例
是
1625
使用附加的验证实例?
否
1635
组合各个验证实例可靠性以产生验证置信级别
1640
填写验证请求

图 16

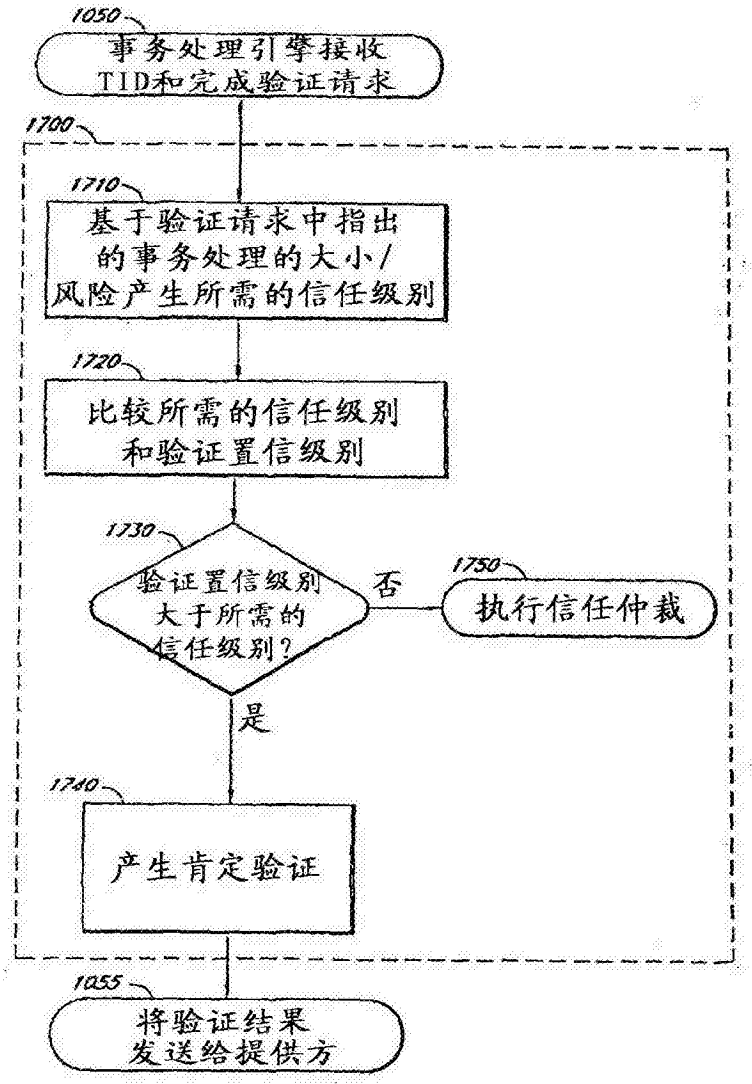

1050
事务处理引擎接收TID和完成验证请求
1700
1710
基于验证请求中指出的事务处理的大小/风险产生所需的信任级别
1720
比较所需的信任级别和验证置信级别
1730
验证置信级别大于所需的信任级别?
否
1750
执行信任仲裁
是
1740
产生肯定验证
1055
将验证结果发送给提供方

图 17

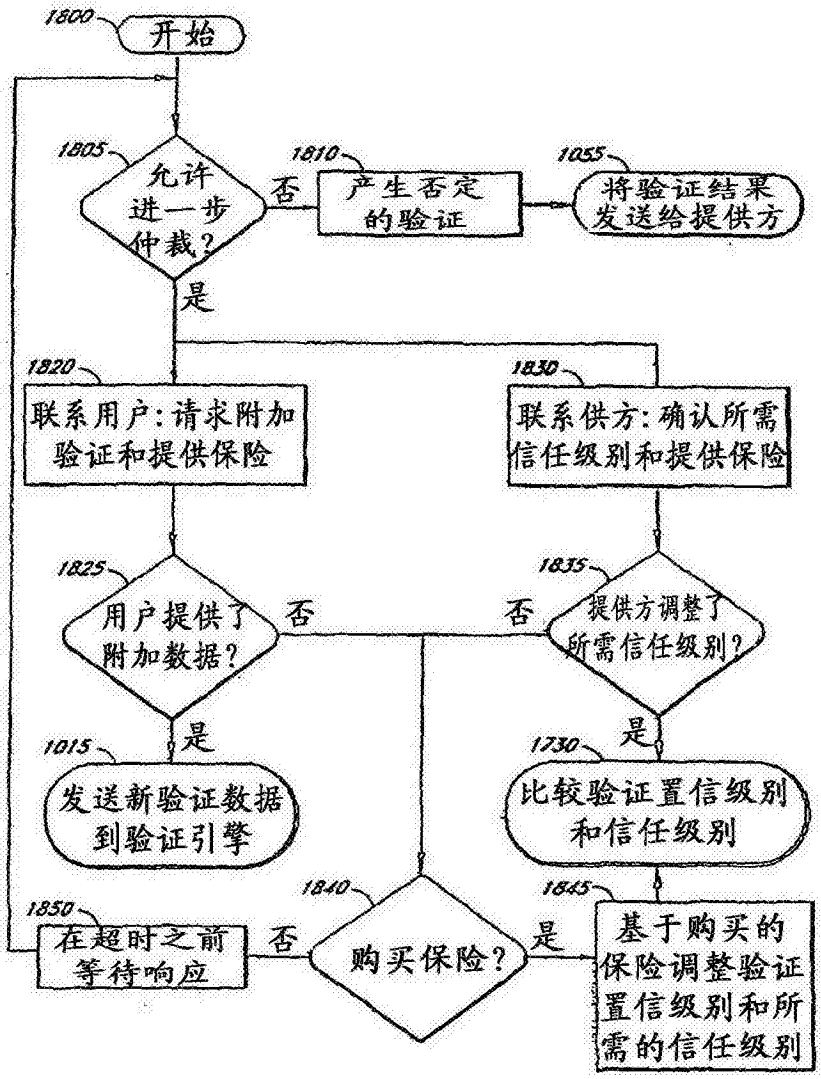

1800
开始
1805
允许进一步仲裁?
否
1810
产生否定的验证
1055
将验证结果发送给提供方
是
1820
联系用户:请求附加验证和提供保险
1830
联系供方:确认所需信任级别和提供保险
1825
用户提供了附加数据?
否
否
1835
提供方调整了所需信任级别?
是
是
1015
发送新验证数据到验证引擎
1730
比较验证置信级别和信任级别
1840
购买保险?
1845
基于购买的保险调整验证置信级别和所需的信任级别
1850
在超时之前等待响应
否
是

图 18

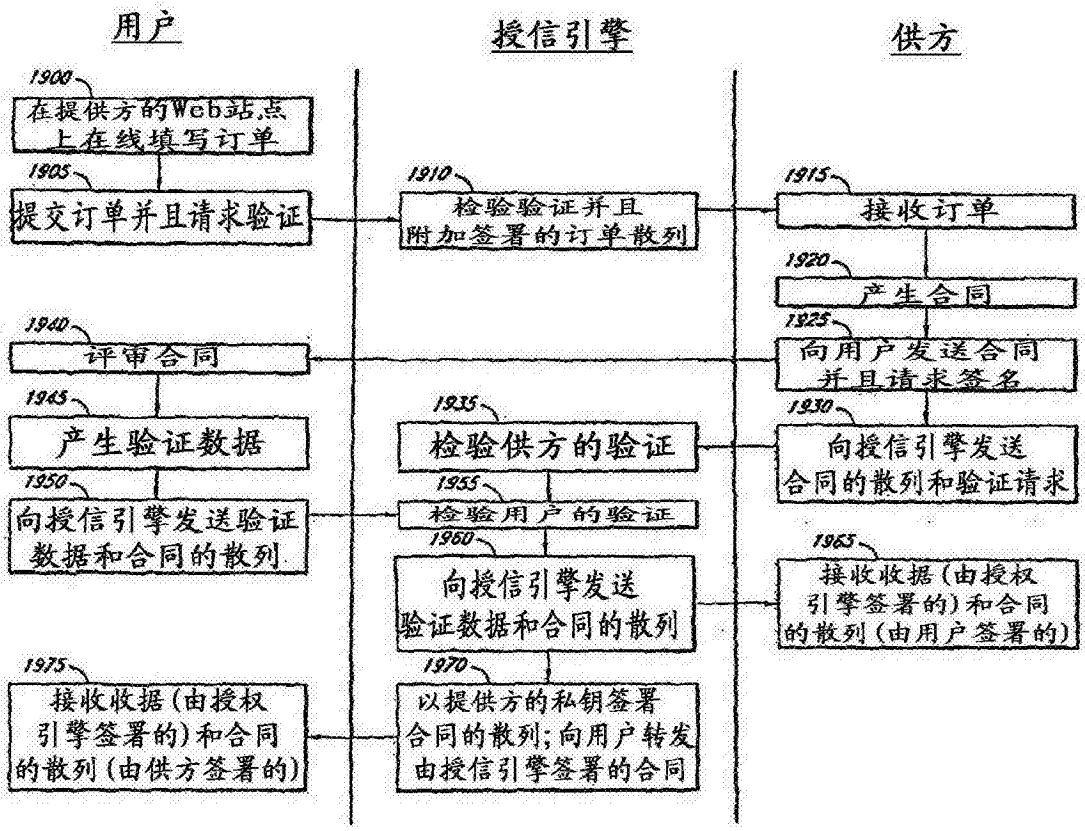

用户
授信引擎
供方
1900
在提供方的Web站点上在线填写订单
1905
提交订单并且请求验证
1910
检验验证并且附加签署的订单散列
1915
接收订单
1920
产生合同
1925
向用户发送合同并且请求签名
1930
向授信引擎发送合同的散列和验证请求
1935
检验供方的验证
1940
评审合同
1945
产生验证数据
1950
向授信引擎发送验证数据和合同的散列
1955
检验用户的验证
1960
向授信引擎发送验证数据和合同的散列
1965
接收收据(由授权引擎签署的)和合同的散列(由用户签署的)
1970
以提供方的私钥签署合同的散列;向用户转发由授信引擎签署的合同
1975
接收收据(由授权引擎签署的)和合同的散列(由供方签署的)

图 19

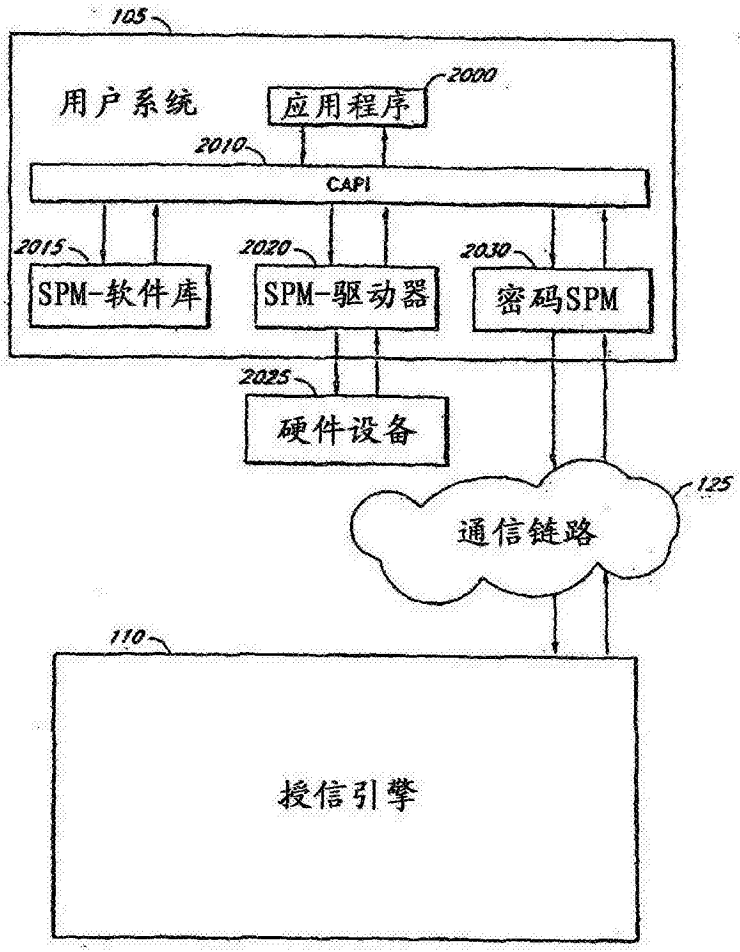

105
用户系统
2000
应用程序
2010
CAPI
2015
SPM-软件库
2020
SPM-驱动器
2030
密码SPM
2025
硬件设备
125
通信链路
110
授信引擎

图 20

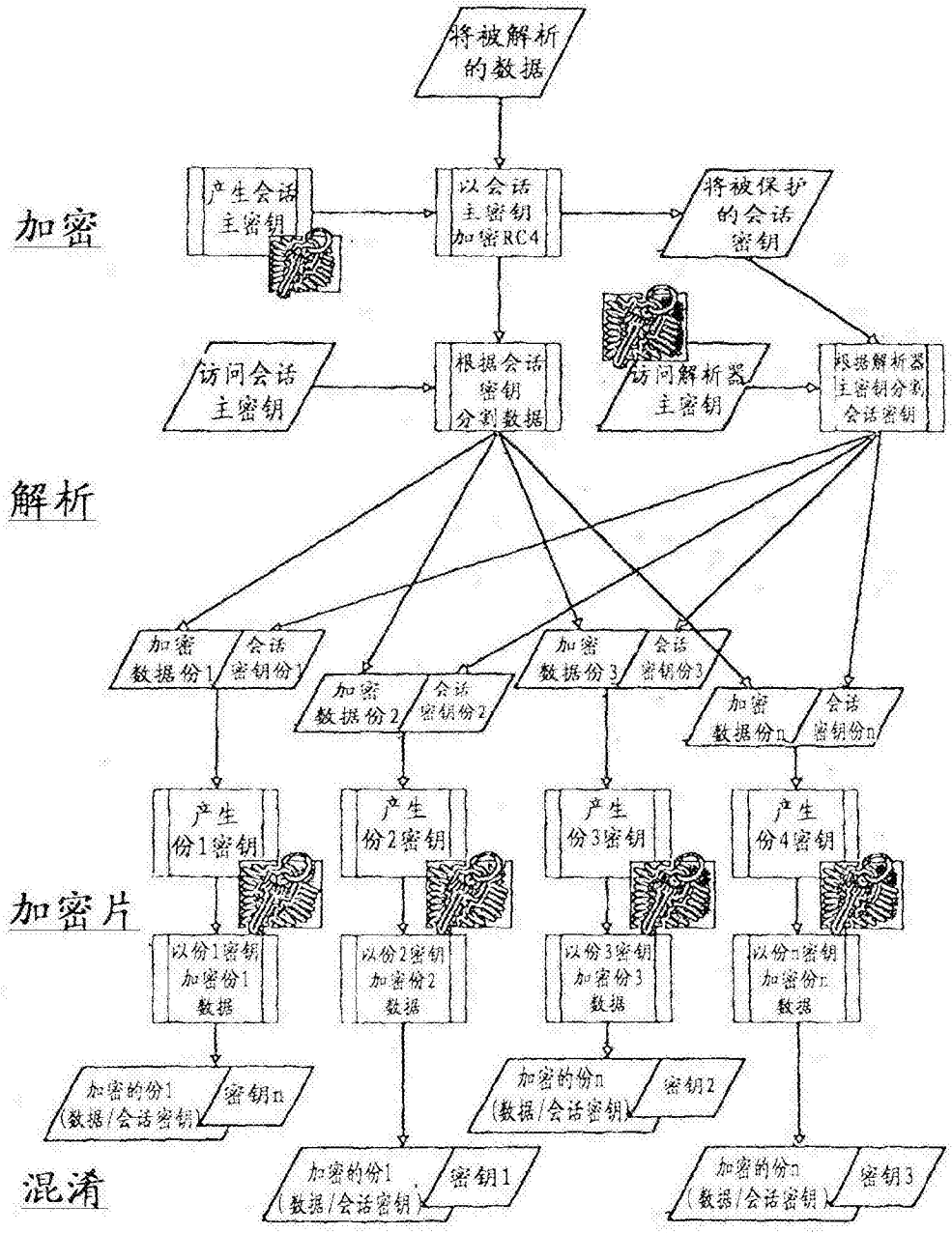

将被解析的数据
加密
产生会话主密钥
以会话主密钥加密RC4
将被保护的会话密钥
访问会话主密钥
根据会话密钥分割数据
访问解析器主密钥
根据解析器主密钥分割会话密钥
解析
加密数据份1
会话密钥份1
加密数据份2
会话密钥份2
加密数据份3
会话密钥份3
加密数据份n
会话密钥份n
产生份1密钥
产生份2密钥
产生份3密钥
产生份4密钥
加密片
以份1密钥加密份1数据
以份2密钥加密份2数据
以份3密钥加密份3数据
以份n密钥加密份n数据
加密的份1(数据/会话密钥)
密钥n
加密的份n(数据/会话密钥)
密钥2
加密的份1(数据/会话密钥)
密钥1
加密的份n(数据/会话密钥)
密钥3
混淆

图 21

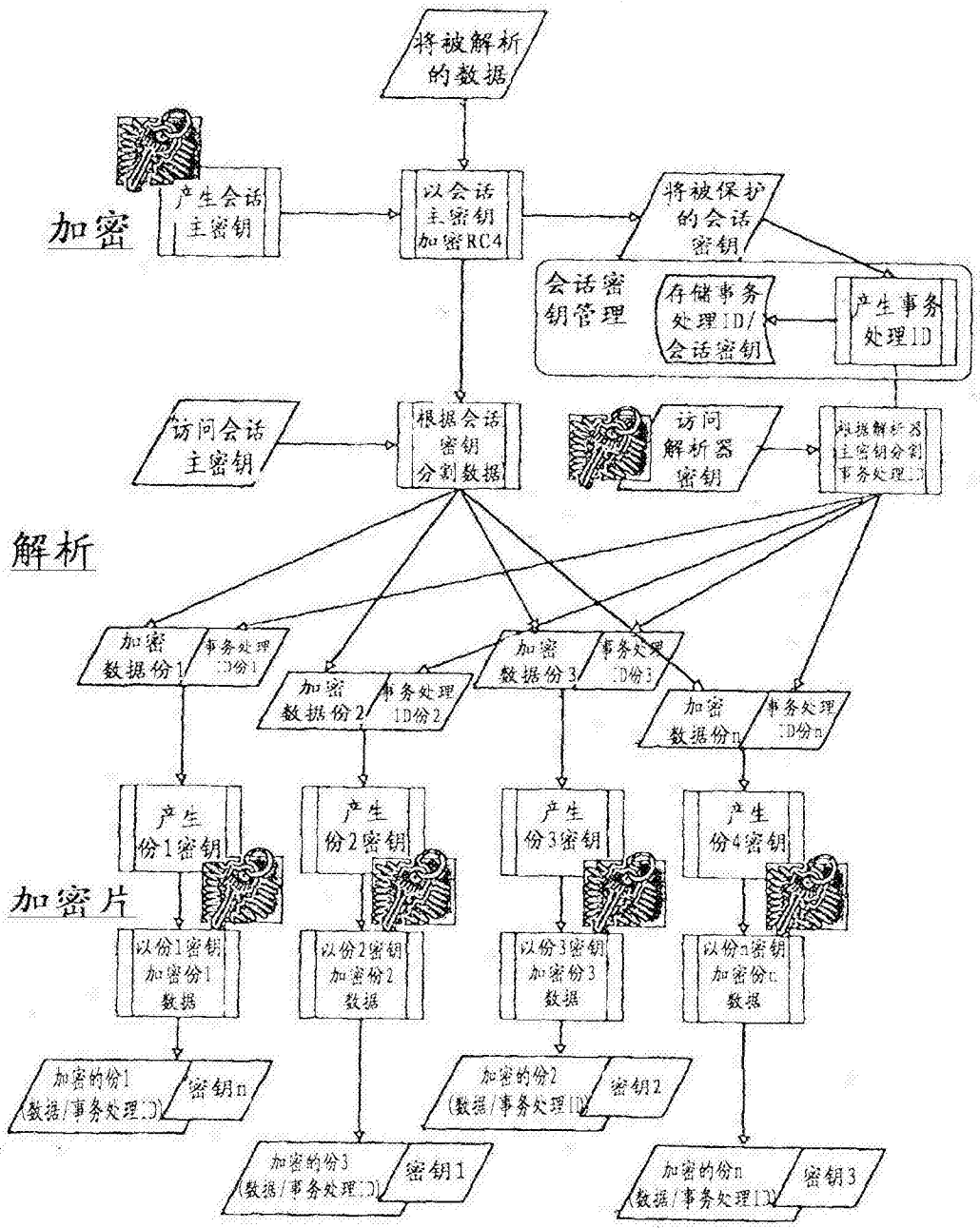

将被解析的数据
加密
产生会话主密钥
以会话主密钥加密RC4
将被保护的会话密钥
会话密钥管理
存储事务处理ID/会话密钥
产生事务处理ID
访问会话主密钥
根据会话密钥分割数据
访问解析器密钥
解析
加密数据份1
事务处理ID份1
加密数据份2
事务处理ID份2
加密数据份3
事务处理ID份3
加密数据份n
事务处理ID份n
产生份1密钥
产生份2密钥
产生份3密钥
产生份4密钥
加密片
以份1密钥加密份1数据
以份2密钥加密份2数据
以份3密钥加密份3数据
以份n密钥加密份n数据
加密的份1(数据/事务处理ID)
密钥n
加密的份2(数据/事务处理ID)
密钥2
加密的份3(数据/事务处理ID)
密钥1
加密的份n(数据/事务处理ID)
密钥3

图 22

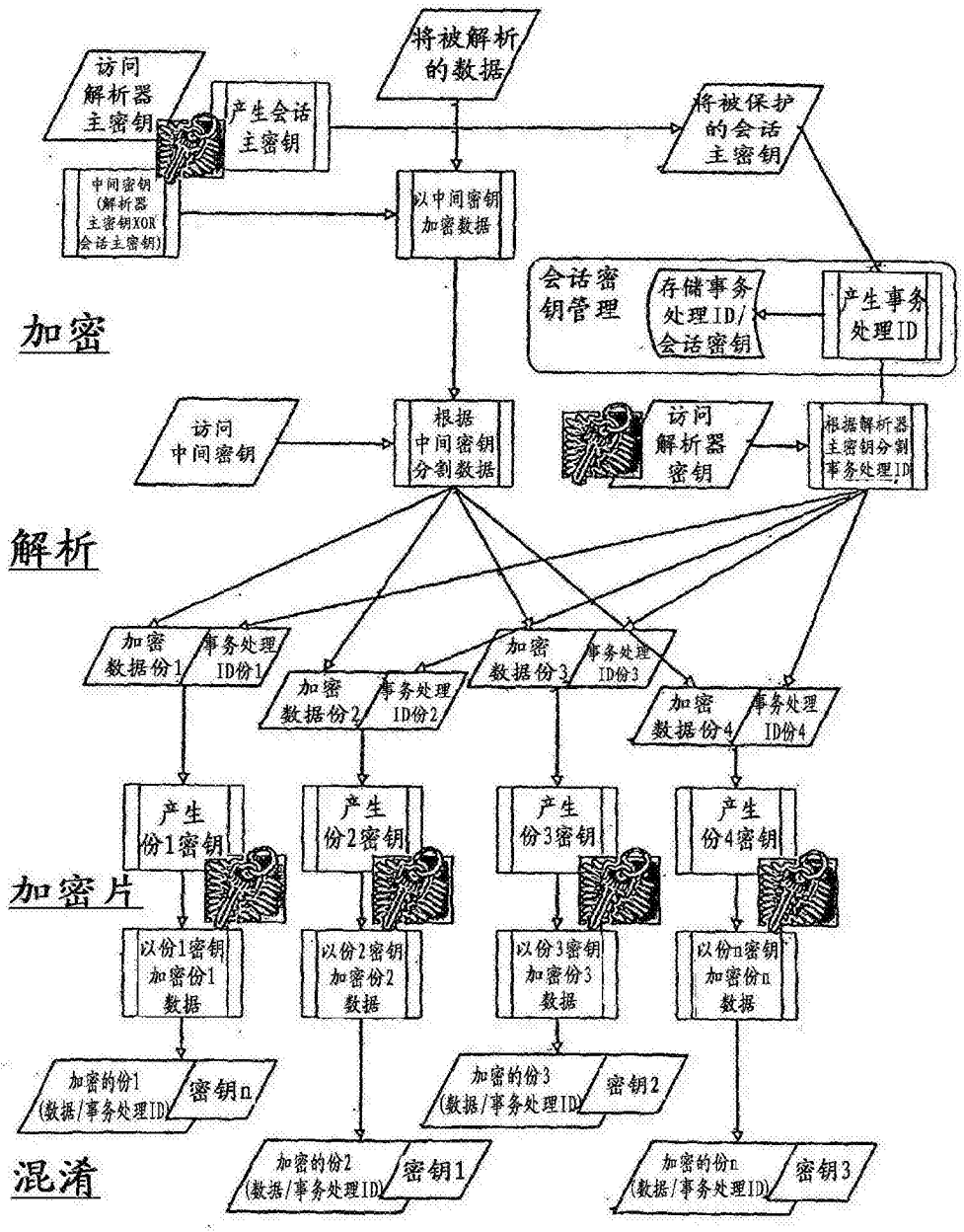

将被解析的数据
访问解析器主密钥
产生会话主密钥
将被保护的会话主密钥
中间密钥(解析器主密钥XOR会话主密钥)
以中间密钥加密数据
会话密钥管理
存储事务处理ID/会话密钥
产生事务处理ID
加密
访问中间密钥
根据中间密钥分割数据
访问解析器密钥
根据解析器主密钥分割事务处理ID
解析
加密数据份1
事务处理ID份1
加密数据份2
事务处理ID份2
加密数据份3
事务处理ID份3
加密数据份4
事务处理ID份4
产生份1密钥
产生份2密钥
产生份3密钥
产生份4密钥
加密片
以份1密钥加密份1数据
以份2密钥加密份2数据
以份3密钥加密份3数据
以份n密钥加密份n数据
加密的份1(数据/事务处理ID)
密钥n
加密的份3(数据/事务处理ID)
密钥2
加密的份2(数据/事务处理ID)
密钥1
加密的份n(数据/事务处理ID)
密钥3
混淆

图 23

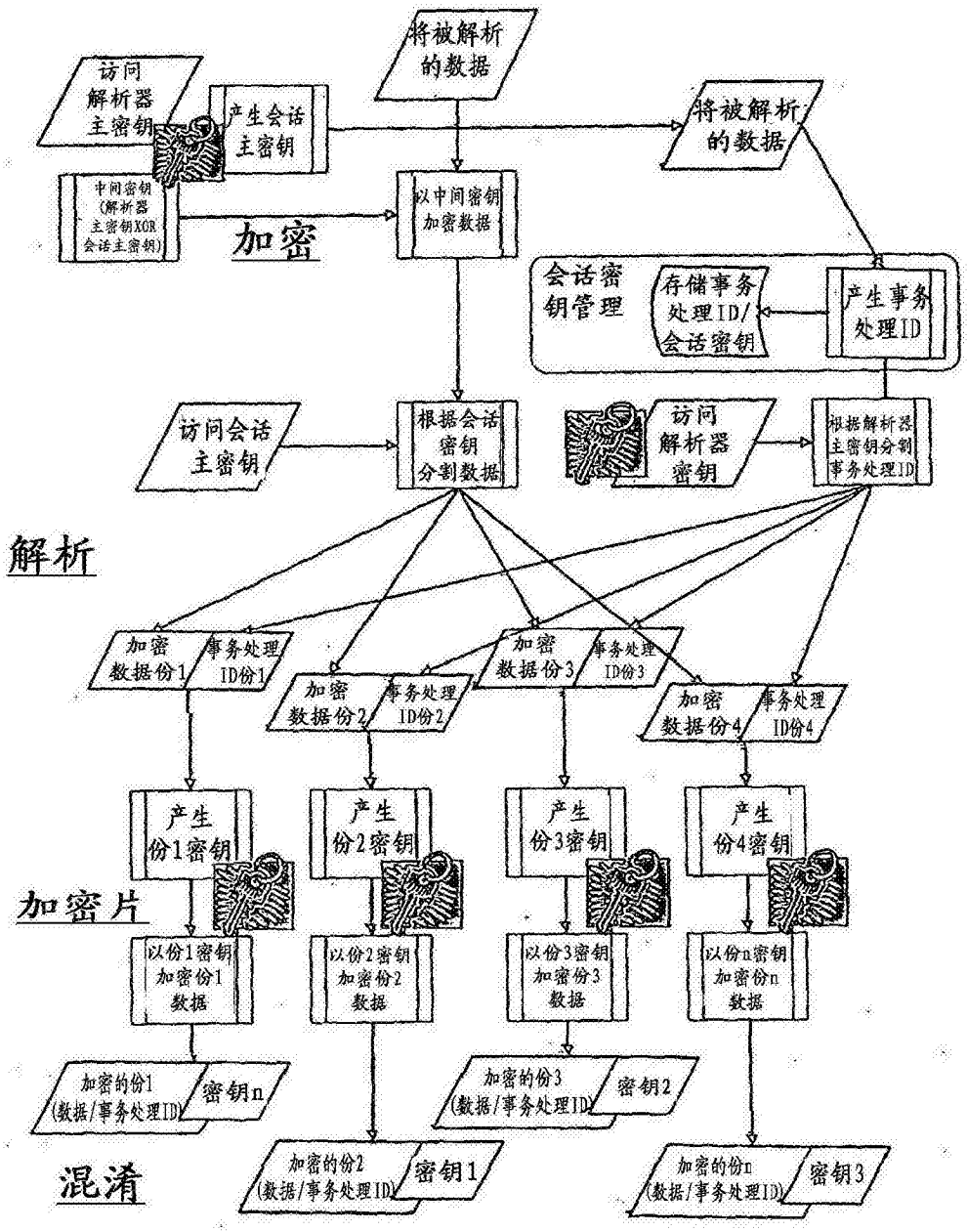

将被解析的数据
访问解析器主密钥
产生会话主密钥
将被解析的数据
中间密钥(解析器主密钥XOR会话主密钥)
以中间密钥加密数据
加密
会话密钥管理
存储事务处理ID/会话密钥
产生事务处理ID
访问会话主密钥
根据会话密钥分割数据
访问解析器密钥
根据解析器主密钥分割事务处理ID
解析
加密数据份1
事务处理ID份1
加密数据份2
事务处理ID份2
加密数据份3
事务处理ID份3
加密数据份4
事务处理ID份4
产生份1密钥
产生份2密钥
产生份3密钥
产生份4密钥
加密片
以份1密钥加密份1数据
以份2密钥加密份2数据
以份3密钥加密份3数据
以份n密钥加密份n数据
加密的份1(数据/事务处理ID)
密钥n
加密的份3(数据/事务处理ID)
密钥2
加密的份2(数据/事务处理ID)
密钥1
加密的份n(数据/事务处理ID)
密钥3
混淆

图 24

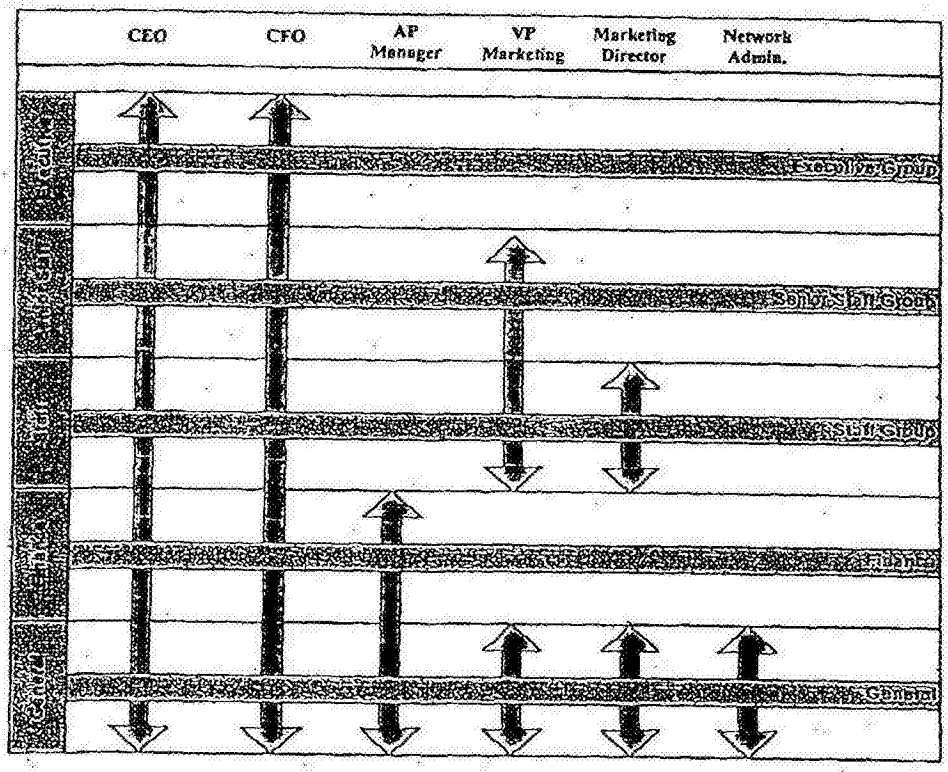

CEO
CFO
AP Manager
VP Marketing
Marketing Director
Network Admin.

图 25

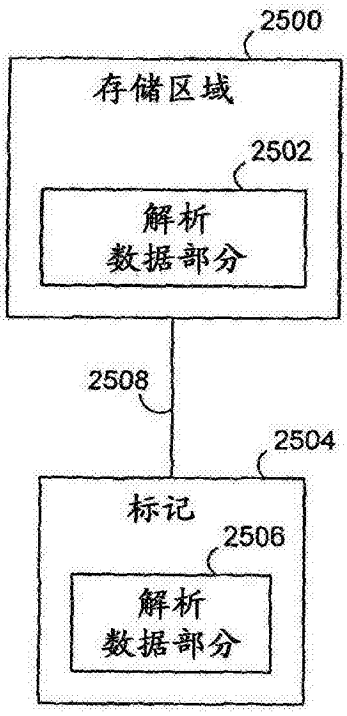

2500
存储区域
2502
解析数据部分
2508
2504
标记
2506
解析数据部分

图 26

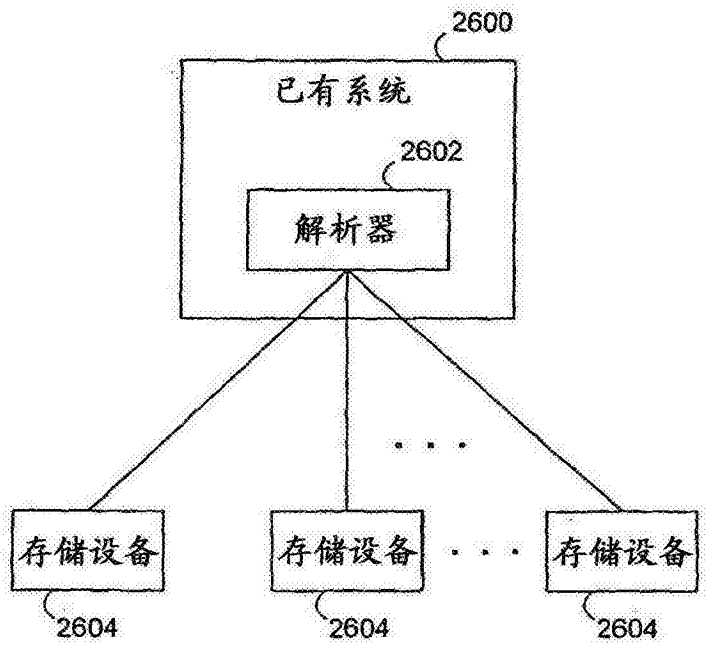

2600
已有系统
2602
解析器
存储设备
2604
存储设备
2604
存储设备
2604

图 27

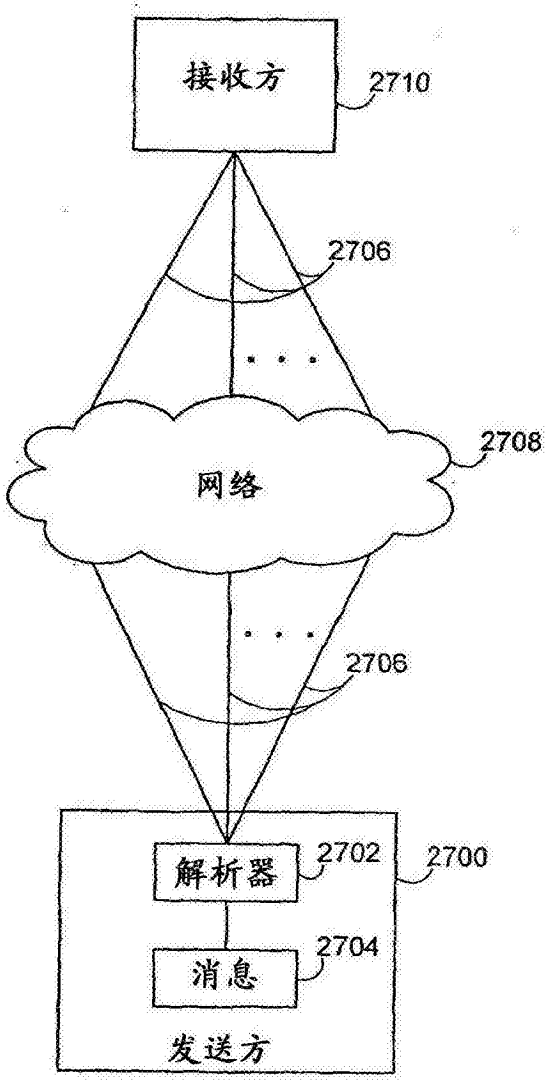

接收方
2710
2706
网络
2708
2706
解析器
2702
2700
消息
2704
发送方

图 28

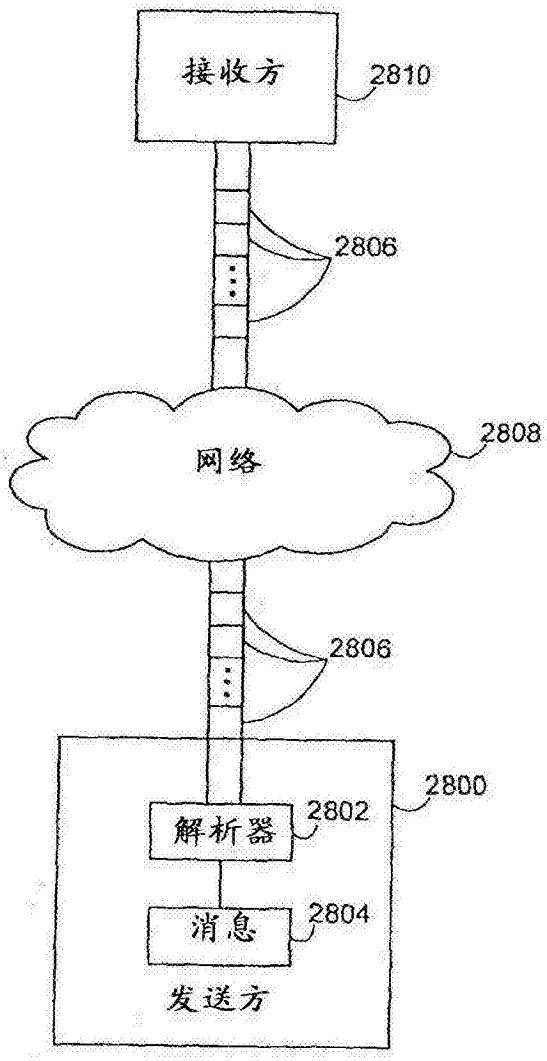

接收方
2810
2806
网络
2808
2806
2800
解析器
2802
消息
2804
发送方

图 29

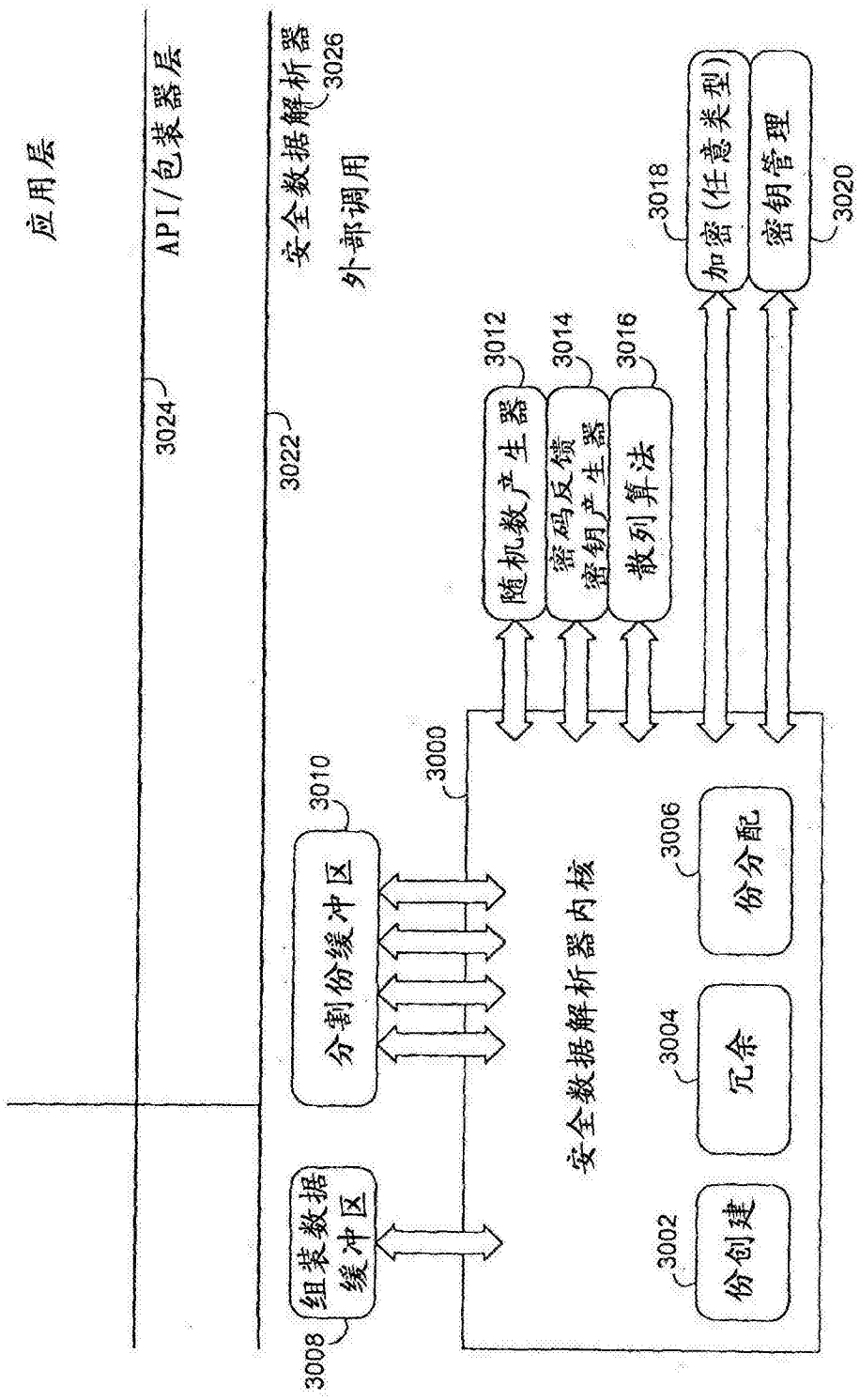

应用层
API/包装器层
安全数据解析器外部调用
3026
3024
3022
3012
随机数产生器
3014
密码反馈密钥产生器
3016
散列算法
3018
加密(任意类型)
密钥管理
3020
3000
安全数据解析器内核
3010
分割份缓冲区
3006
份分配
3004
冗余
3002
份创建
3008
组装数据缓冲区

图 30

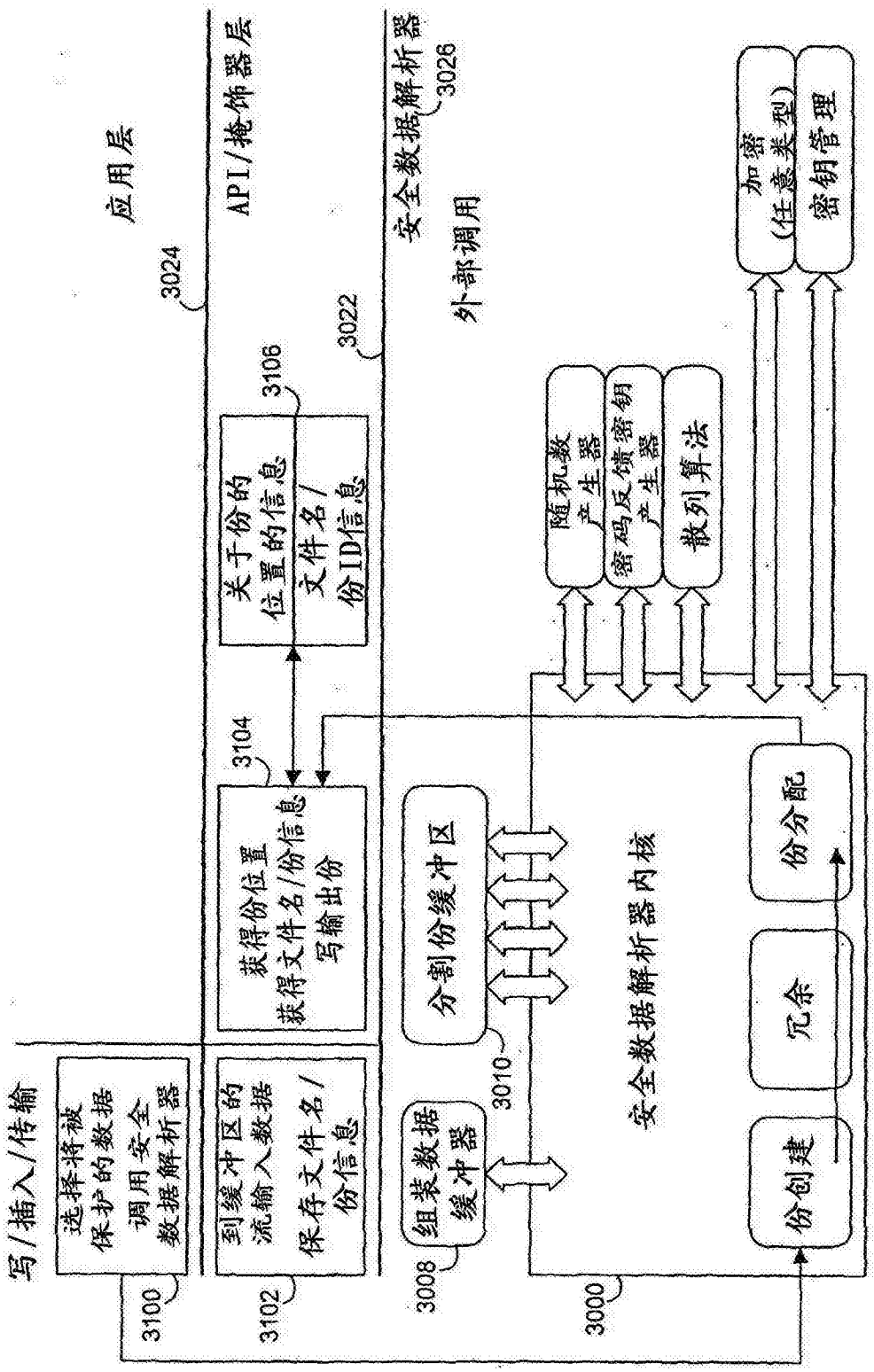

写/插入/传输
应用层
API/掩饰器层
安全数据解析器
3026
外部调用
3024
3022
选择将被保护的数据调用安全数据解析器
3100
到缓冲区的流输入数据保存文件名/份信息
3102
获得份位置获得文件名/份信息写输出份
3104
关于份的位置的信息
文件名/份ID信息
3106
分割份缓冲区
组装数据缓冲器
3008
3010
安全数据解析器内核
3000
随机数产生器
密码反馈密钥产生器
散列算法
加密(任意类型)
密钥管理
份分配
冗余
份创建

图 31

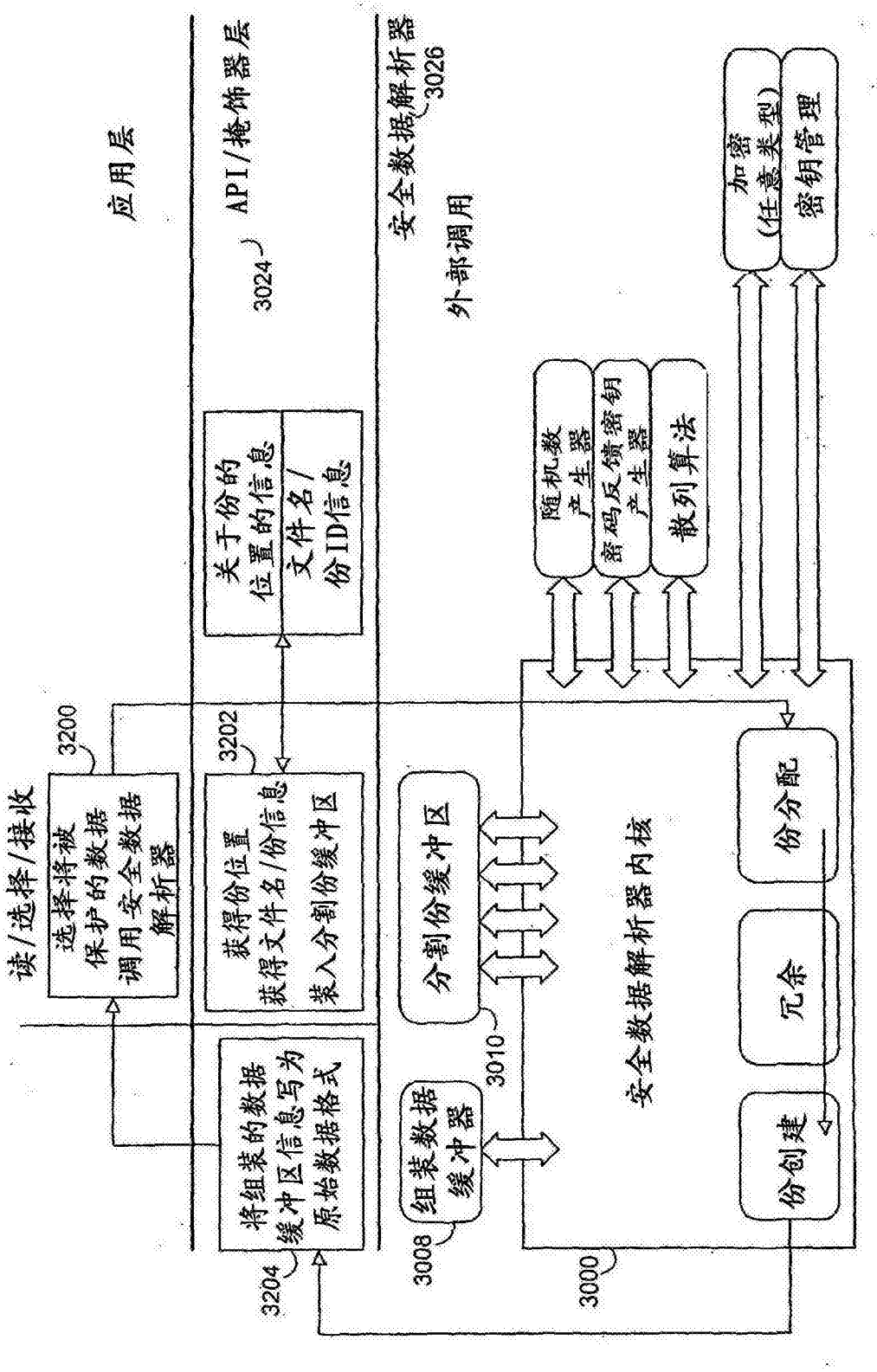

应用层
API/掩饰器层
3024
安全数据解析器
3026
外部调用
读/选择/接收
选择将被保护的数据调用安全数据解析器
3200
获得份位置
获得文件名/份信息
装入分割份缓冲区
3202
关于份的位置的信息
文件名/份ID信息
将组装的数据缓冲区信息写为原始数据格式
3204
分割份缓冲区
3010
组装数据缓冲器
3008
安全数据解析器内核
3000
随机数产生器
密码反馈密钥产生器
散列算法
加密(任意类型)
密钥管理
份分配
冗余
份创建

图 32

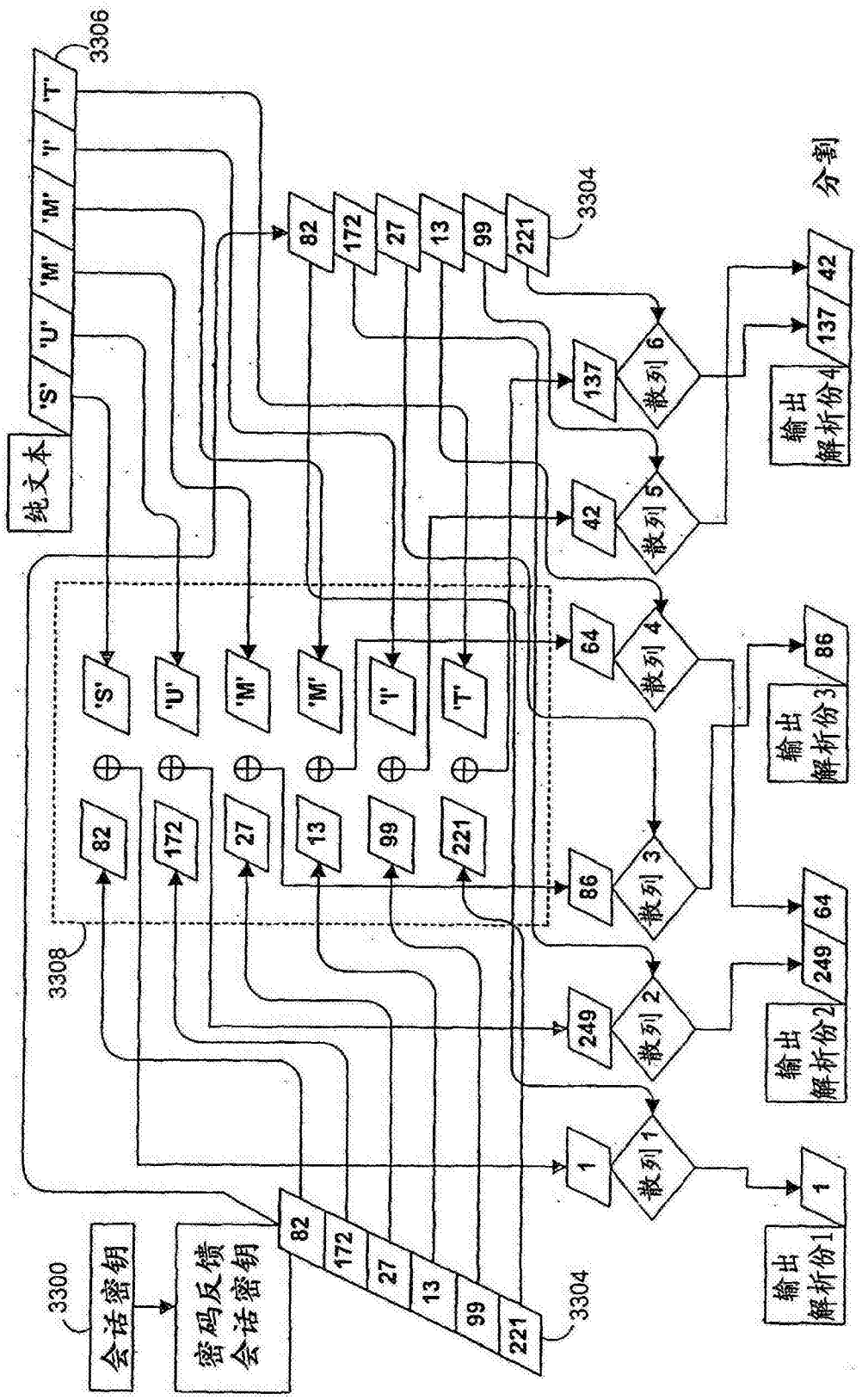

3306
纯文本
'S' 'U' 'M' 'M' 'I' 'T'
3304
82 172 27 13 99 221
3308
会话密钥
3300
密码反馈会话密钥
散列 1
散列 2
散列 3
散列 4
散列 5
散列 6
输出解析份1
输出解析份2
输出解析份3
输出解析份4
分割

图 33

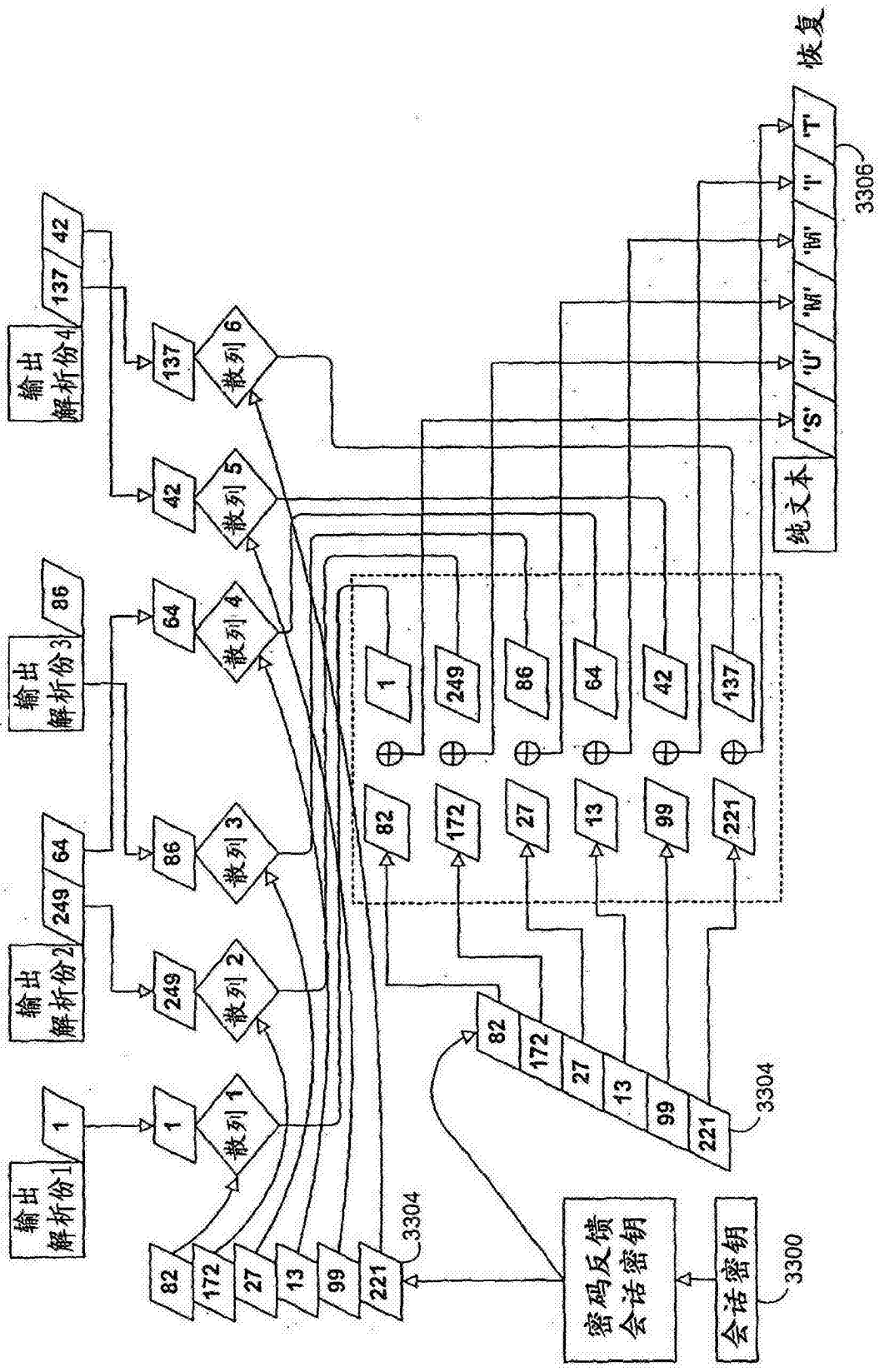

输出解析份1
输出解析份2
输出解析份3
输出解析份4
散列 1
散列 2
散列 3
散列 4
散列 5
散列 6
密码反馈会话密钥
会话密钥
3300
3304
3306
恢复
纯文本
'S'
'U'
'B'
'B'
'I'
'T'

图 34

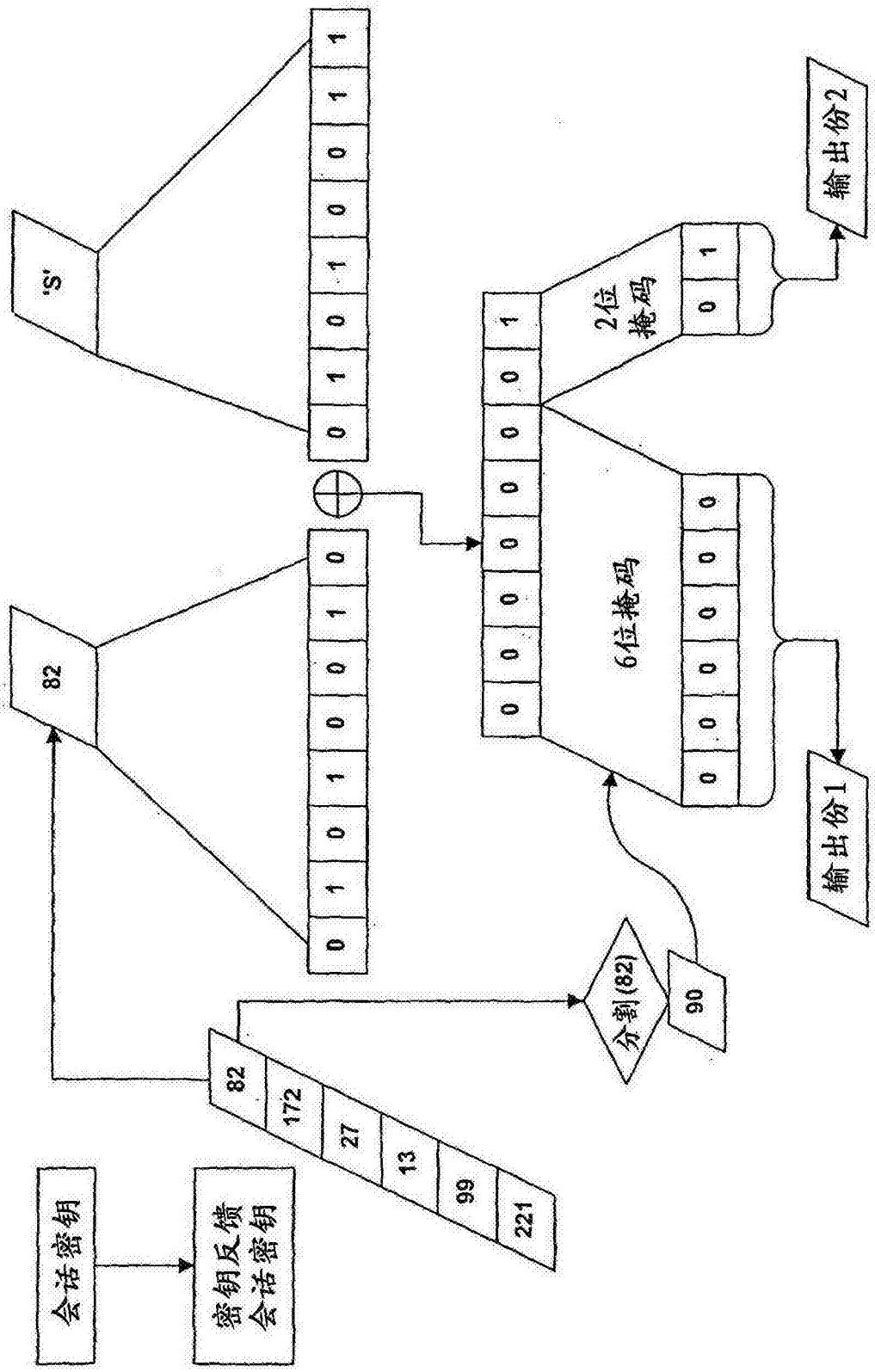

会话密钥
密钥反馈
会话密钥
82
172
27
13
99
221
分割(82)
90
82
'S'
6位掩码
2位
掩码
输出份1
输出份2

图 35

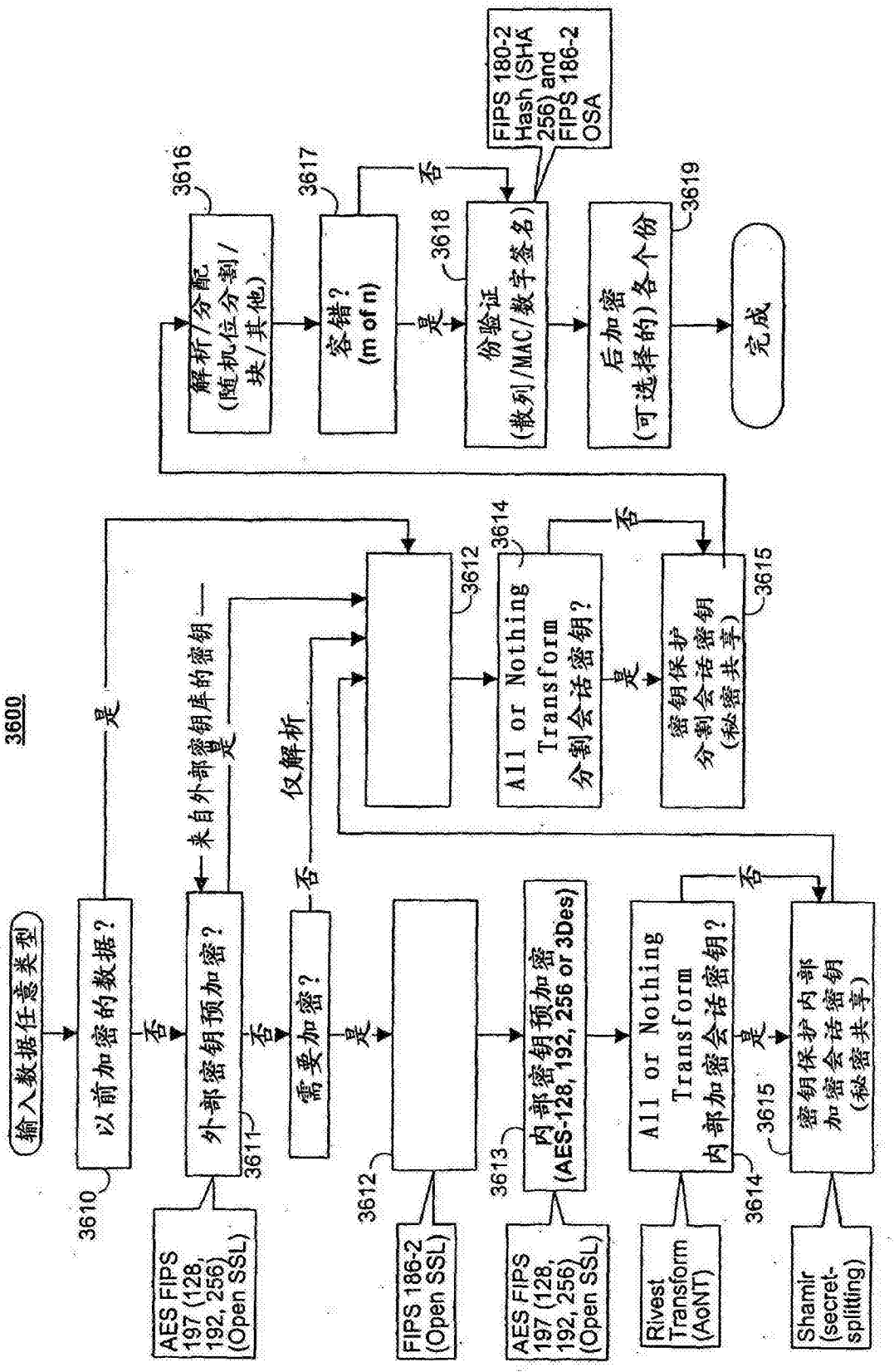

3600
输入数据任意类型
以前加密的数据？
是
否
外部密钥预加密？
来自外部密钥库的密钥
是
否
需要加密？
是
否
仅解析
All or Nothing Transform 分割会话密钥？
是
否
密钥保护 分割会话密钥 (秘密共享)
内部密钥预加密 (AES-128, 192, 256 or 3Des)
All or Nothing Transform 内部加密会话密钥？
是
否
密钥保护内部加密会话密钥 (秘密共享)
3610
3611
3612
3613
3614
3615
AES FIPS 197 (128, 192, 256) (Open SSL)
FIPS 186-2 (Open SSL)
AES FIPS 197 (128, 192, 256) (Open SSL)
Rivest Transform (AoNT)
Shamir (secret-splitting)
3616
解析/分配 (随机位分割/块/其他)
3617
容错？ (m of n)
否
是
3618
份验证 (散列/MAC/数字签名)
FIPS 180-2 Hash (SHA 256) and FIPS 186-2 OSA
3619
后加密 (可选择的)各个份
完成

图 36

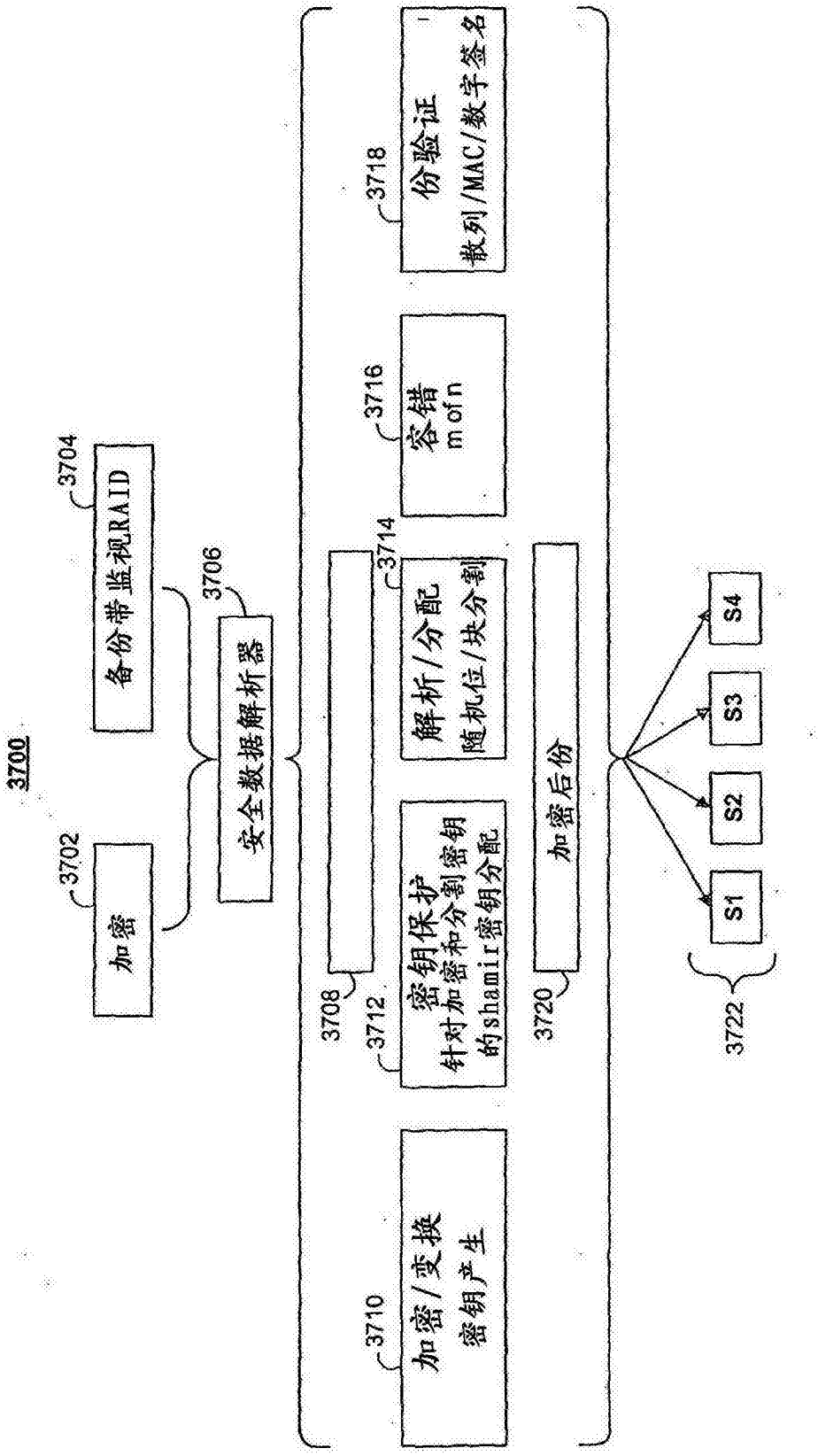

3700
3702
加密
3704
备份带监视RAID
3706
安全数据解析器
3708
3710
加密/变换
密钥产生
3712
密钥保护
针对加密和分割密钥
的shamir密钥分配
3714
解析/分配
随机位/块分割
3716
容错
m of n
3718
份验证
散列/MAC/数字签名
3720
加密后份
3722
S1
S2
S3
S4

图 37

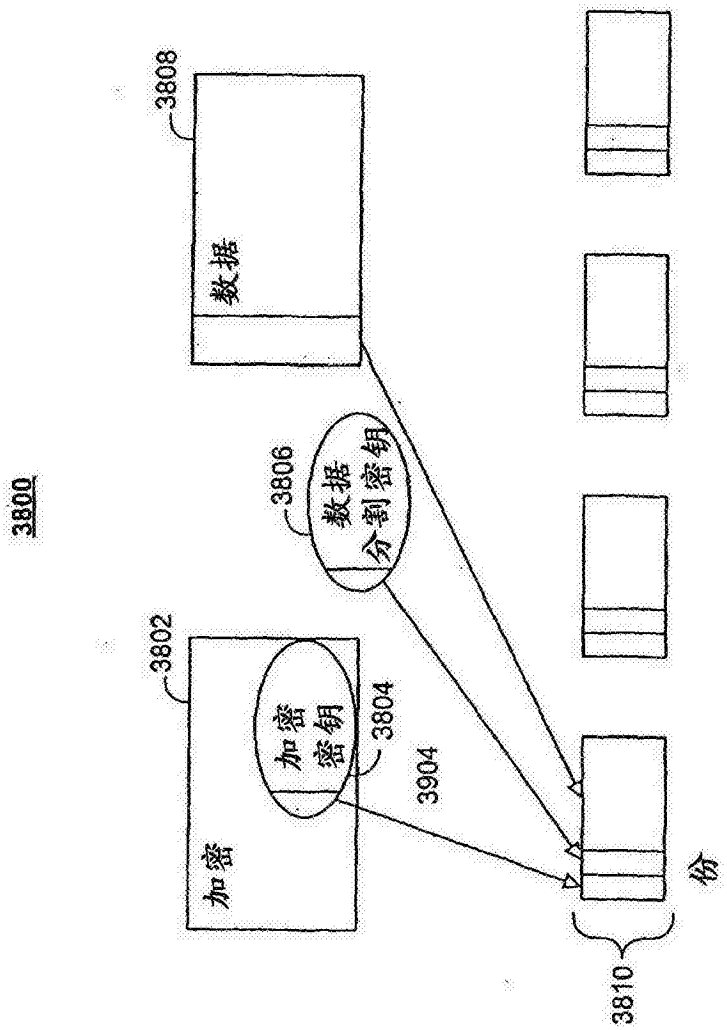



图 38

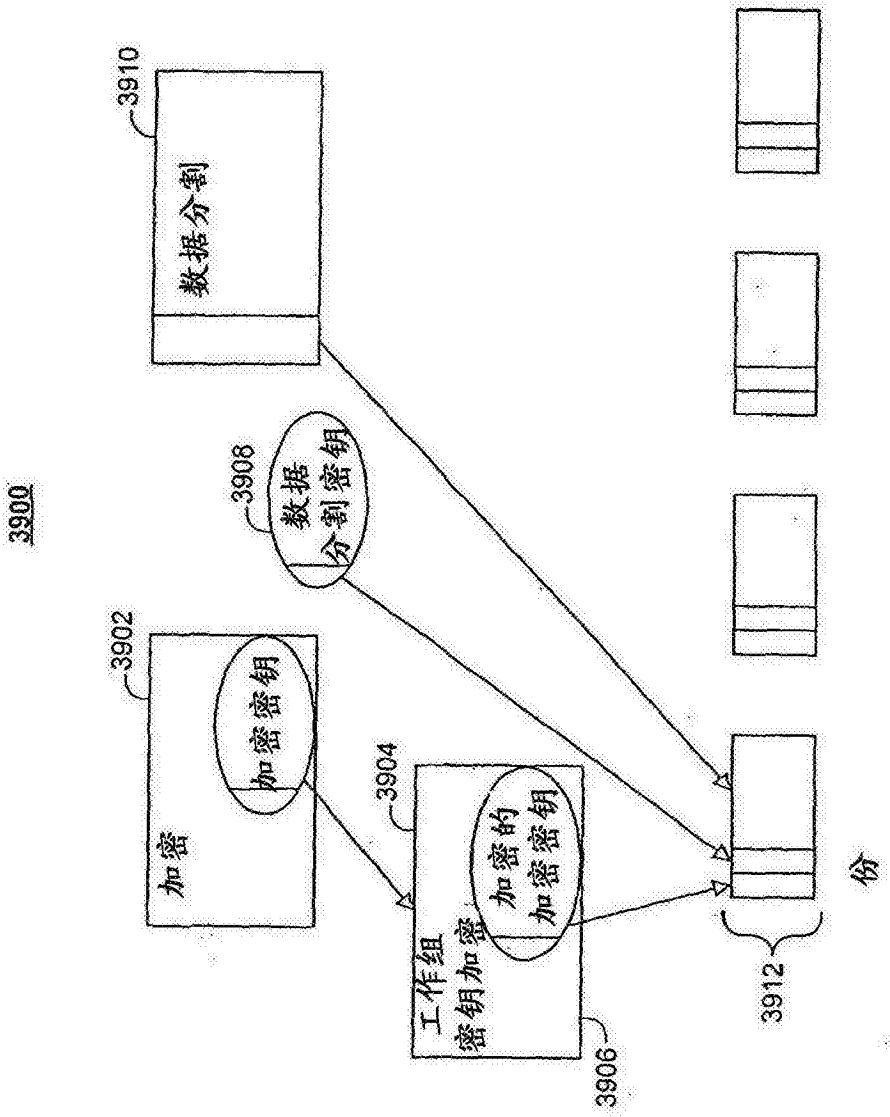

3900
3910
数据分割
3908
数据分割密钥
3902
加密
加密密钥
3904
工作组密钥加密
加密的加密密钥
3906
3912
份

图 39

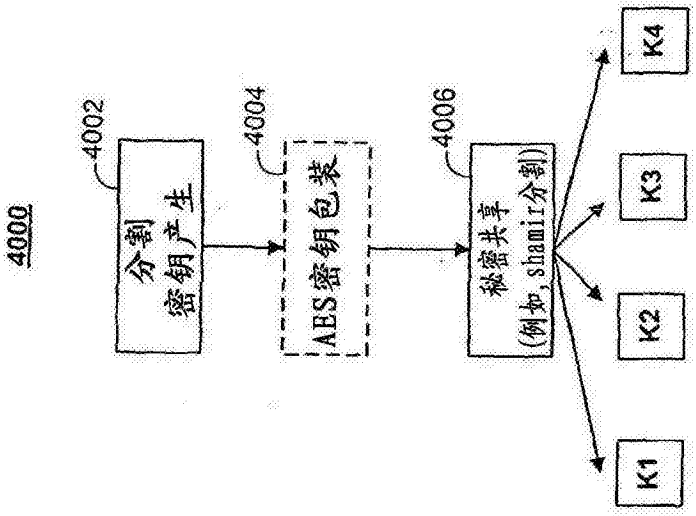

4000
4002
分割密钥产生
4004
AES密钥包装
4006
秘密共享(例如,shamir分割)
K4
K3
K2
K1

图 40A

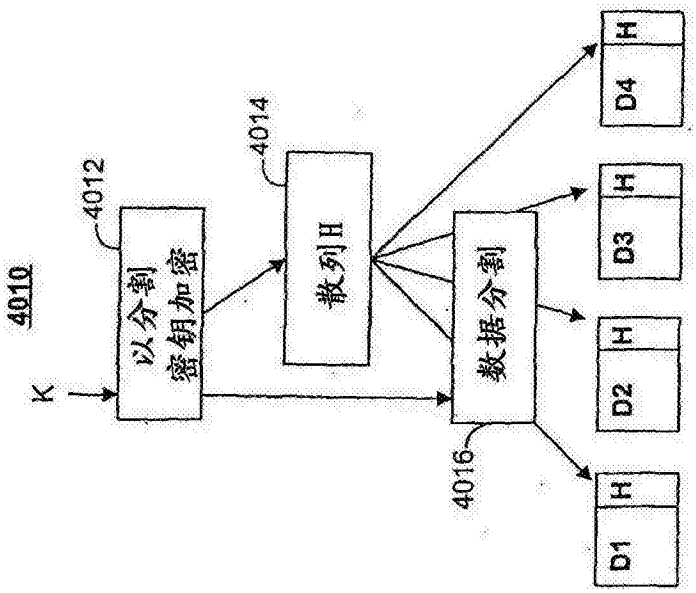

4010
K
4012
以分割密钥加密
4014
散列H
数据分割
4016
H
D4
H
D3
H
D2
H
D1

图 40B

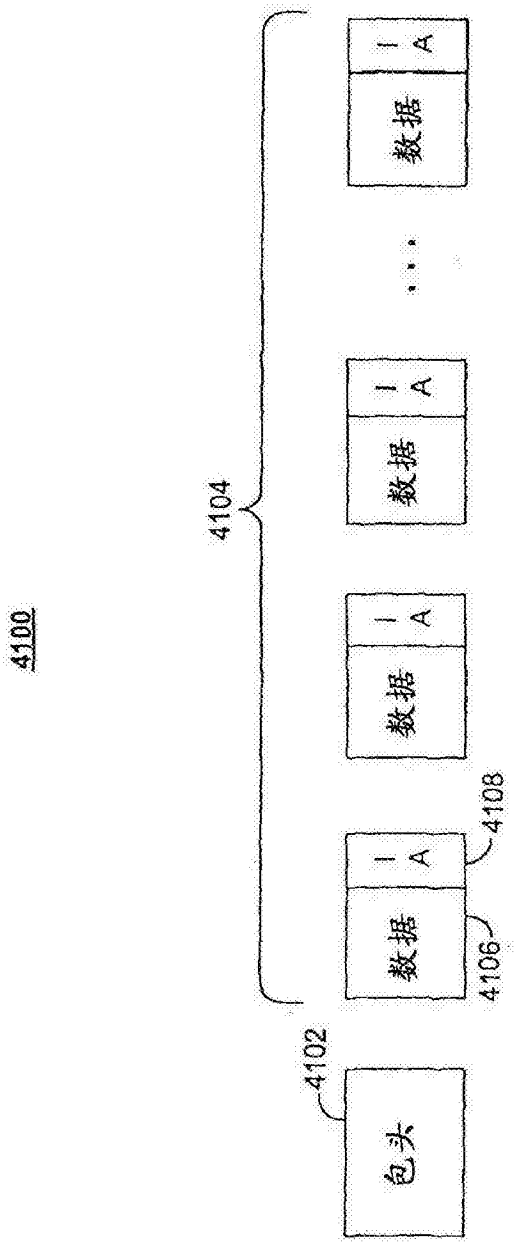



图 41