



[12] 发明专利申请公开说明书

[21] 申请号 01820944.0

[43] 公开日 2004年3月10日

[11] 公开号 CN 1481525A

[22] 申请日 2001.10.15 [21] 申请号 01820944.0

[30] 优先权

[32] 2000.10.20 [33] US [31] 09/693,605

[86] 国际申请 PCT/US01/32089 2001.10.15

[87] 国际公布 WO02/35329 英 2002.5.2

[85] 进入国家阶段日期 2003.6.20

[71] 申请人 伊露西斯有限公司

地址 美国堪萨斯州

[72] 发明人 A·马杜赫

[74] 专利代理机构 上海专利商标事务所

代理人 李家麟

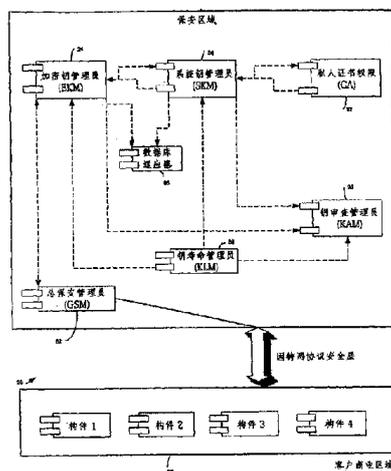
权利要求书 11 页 说明书 19 页 附图 8 页

[54] 发明名称 隐藏链路动态密钥管理员用于电脑系统有数据库结构作储存加密数据及作储存及撷取加密数据的方法

[57] 摘要

一电脑系统(20)有一保安区域(22)、至少一用户商业区域(26)、及一重复用户终端机(34)使用一隐藏链路动态密钥管理员(24、84)及一包括数据实体(30C, 30D)的数据库结构及一保安密钥识别属性(32)作加密数据的储存。一于电脑系统(20)中加密、储存、解码及撷取加密资料操作的方法,包括一资料数据库(62)及一密钥数据库(44)。密钥数据库(44)是与资料数据库(62)分离的。保安区域(22)包括一系统密钥管理员(84)可用以产生有系统密钥共同名称的系统密钥及一加密密钥管理员(24)可用以产生有加密密钥识别的加密密钥。密钥管理员(24, 84)操作于一密钥伺服器(40),那是由一次密钥伺服器(42)所反射。一总保安管理员(82)也是操作于一密钥伺服器(40)以控制保安区域(22)的存取。保安资料属性(32)是与一持续数据实体(30A)一起储存,那是相关于其他的数据实体(30C, 30D)。保安资料属性(32)包括用以加密数据实体(30C, 30D)的加密钥

识别(112)。加密钥识别是由系统密钥加密,及系统密钥共同名称散列值也是储存于保安资料属性(32)。资料数据实体(30)是储存于资料数据库(62),但加密钥识别(153)、加密钥(154)、系统密钥共同名称散列值(156, 157)、及系统密钥共同名称(158)是储存于在保安区域(22)中密钥数据库(44)之中。系统密钥本身是储存于一在保安区域中的灵巧卡阅读器(56)。



1. 一电脑可读媒介包括一作储存加密数据的数据库结构，数据库结构包括：以至少一加密钥加密的至少一数据实体，数据实体有至少一个可搜索的属性；及至少一与数据实体相关及对应于加密钥的加密钥识别。
2. 根据权力要求 1 的电脑可读媒介，当中至少一加密钥识别是以一系统钥加密，及数据库结构进一步包括一对应于系统钥的系统钥共同名称，及系统钥共同名称是相关于数据实体地被储存。
3. 根据权力要求 2 的电脑可读媒介，当中系统钥共同名称是被散列，及数据库结构进一步包括一是相关于系统共同名称地被储存的系统钥共同名称散列值。
4. 根据权力要求 3 的电脑可读媒介，当中系统钥共同名称及系统钥共同名称散列值是被储存于一与至少一数据实体分离的数据库。
5. 根据权力要求 1 的电脑可读媒介，当中至少一加密钥识别是以一系统钥加密。
6. 根据权力要求 1 的电脑可读媒介，当中至少一加密钥包括一动态加密钥，及至少一加密钥识别包括一动态加密钥识别。
7. 根据权力要求 1 的电脑可读媒介进一步包括一以一重复的加密钥加密的重复的数据实体，及一重复的加密钥识别。
8. 根据权力要求 7 的电脑可读媒介，当中重复的加密钥包括动态加密钥，及重复的加密钥识别包括动态加密钥识别。
9. 根据权力要求 1 的电脑可读媒介，当中数据库结构进一步包括一与每一个的可搜索属性有一相对应的散列值的重复的散列值。
10. 根据权力要求 1 的电脑可读媒介，当中数据库结构进一步包括至少一与数据实体相关的完整的属性。
11. 根据权力要求 1 的电脑可读媒介，当中数据库结构进一步包括一数据实体的保安钥属性，保安钥属性包括至少一加密钥识别及一系统钥共同名称。
12. 根据权力要求 1 的电脑可读媒介，进一步包括一第一数据库包括数据实体及储存在其上的加密钥识别和一包括储存在其上的加密钥的第二数据库。

13. 根据权力要求 12 的电脑可读媒介，当中第一数据库进一步包括一储存在其上的系统钥共同名称，及对应于一用作加密加密钥识别的系统钥的系统钥共同名称。

14. 根据权力要求 13 的电脑可读媒介，进一步包括一包括储存在其上的系统钥的保安令牌。

15. 根据权力要求 14 的电脑可读媒介，当中保安令牌包括一灵巧卡阅读器。

16. 根据权力要求 1 的电脑可读媒介，当中至少一加密钥识别是以一数据实体的属性储存。

17. 根据权力要求 1 的电脑可读媒介，当中数据实体包括一有一重复属性的数据物件。

18. 根据权力要求 1 的电脑可读媒介，进一步包括一第二数据实体包括如加密钥及加密钥识别属性。

19. 根据权力要求 18 的电脑可读媒介，当中第二数据实体是储存于一与至少一数据实体分离的数据库。

20. 根据权力要求 1 的电脑可读媒介，进一步包括一以第二加密钥加密的第二数据实体，第二数据实体有一第二可搜索属性，及一对应于第二加密钥的第二加密钥识别，及当中至少一加密钥包括一第一加密钥及至少一包括一第一加密钥识别的加密钥识别。

21. 根据权力要求 20 的电脑可读媒介，当中第二加密钥识别是以一第二数据实体属性储存。

22. 根据权力要求 20 的电脑可读媒介，当中第一及第二加密钥识别是以一有一系统钥共同名称的系统钥加密。

23. 根据权力要求 22 的电脑可读媒介，当中系统钥包括一共同系统钥。

24. 根据权力要求 22 的电脑可读媒介，进一步包括系统钥共同名称是以第一及第二数据实体属性储存。

25. 根据权力要求 20 的电脑可读媒介，当中第一加密钥识别是以一第一系统钥加密，及第二加密钥识别是以一第二系统钥加密。

26. 根据权力要求 20 的电脑可读媒介，当中第一及第二数据实体包含个别客户资料。

27. 根据权力要求 26 的电脑可读媒介，当中第一数据实体包含病人名称资料，及第二数据实体包含病人地址资料。

28. 一电脑可读数据传输媒介包含一作加密数据的数据结构，数据结构包括：

以至少一加密钥加密的至少一数据实体，数据实体有至少一个可搜索的属性；及

至少一与数据实体相关及对应于加密钥的加密钥识别。

29. 一电脑可读数据传输媒介包含一作加密数据的数据结构，数据结构包括：

以至少一有一加密钥识别的加密钥加密的一重复数据实体；及

至少一对应于用作加密加密钥识别的系统钥的系统钥共同名称。

30. 一电脑可读媒介包含一作储存加密数据的数据库结构，数据库结构包括：

以至少一有一加密钥识别的加密钥加密的一重复数据实体；及

至少一对应于用作加密加密钥识别的系统钥的系统钥共同名称。

31. 根据权力要求 30 的电脑可读媒介，当中数据结构进一步包括加密钥识别。

32. 根据权力要求 31 的电脑可读媒介，当中加密钥识别是以系统钥加密。

33. 根据权力要求 30 的电脑可读媒介，当中重复数据实体包括一以至少一加密钥加密的第一数据实体及一以第二加密钥加密的第二数据实体，及进一步包括一对应于至少一加密钥的第一加密钥识别及一对应于第二加密钥的第二加密钥识别。

34. 根据权力要求 33 的电脑可读媒介，当中系统钥共同名称包括一对应于第一系统钥的第一系统钥共同名称，及数据结构进一步包括加密钥识别，那是一被第一系统钥加密的第一加密钥识别，及一对应于第二系统钥的第二系统钥共同名称，及当中第二加密钥识别是以第二系统钥加密。

35. 根据权力要求 33 的电脑可读媒介，当中复数据实体包括一以第三加密钥加密的第三数据实体，及进一步包括一对应于第三加密钥的第三加密钥识别。

36. 根据权力要求 35 的电脑可读媒介，当中第一、第二、及第三数据实体有关于一个人的，第一数据实体包含个人的名称资料，第二数据实体包含个人的地址资料，及第三数据实体包含个人的电话资料。

37. 根据权力要求 30 的电脑可读媒介，当中系统钥共同名称是散列的。

38. 根据权力要求 37 的电脑可读媒介进一步包括一系统钥数据实体包括系统钥共同名称及统钥共同名称散列值。

39. 根据权力要求 38 的电脑可读媒介，当中重复数据实体是储存于一第一数据库，及系统钥数据实体是储存于一第二数据库。

40. 一种储存及撷取加密数据的方法，此方法包括：

使用一有一加密钥识别的加密钥加密数据实体；储存数据实体；及以关联于数据实体地储存加密钥识别。

41. 根据权力要求 40 的方法进一步包括：

使用一可搜索属性以要求数据操作；

搜索与可搜索属性所相配的；

使用一加密钥识别搜索加密钥；

以加密钥解码数据实体。

42. 根据权力要求 41 的方法，当中要求数据操作包括要求一新资料的数据更新，及进一步包括以一第二加密钥加密新资料。

43. 根据权力要求 41 的方法，当中要求数据操作包括要求一新资料的增加，及进一步包括以一第二加密钥加密新资料。

44. 根据权力要求 41 的方法，当中要求数据操作包括要求检阅现时的资料，及进一步包括以一第二加密钥加密检阅的资料。

45. 根据权力要求 40 的方法，进一步包括以一有一系统钥共同名称的系统钥加密加密钥识别。

46. 根据权力要求 45 的方法，进一步包括储存系统钥于一保安令牌。

47. 根据权力要求 45 的方法进一步包括：

使用一可搜索属性以要求数据操作；

搜索与可搜索属性所相配的；

使用一系统钥共同名称搜索系统钥；

以系统钥解码加密钥识别；

使用一加密钥识别搜索加密钥；

以加密钥解码数据实体。

48. 根据权力要求 45 的方法，当中包括使用一以系统共同钥加密的加密钥识别的系统钥加密的加密钥识别。

49. 根据权力要求 48 的方法，进一步包括以一系统个人密码解码加密钥识

别。

50. 根据权力要求 45 的方法，进一步包括以关联于数据实体地储存系统钥共同名称。

51. 根据权力要求 45 的方法，进一步包括检查系统钥期限，及当系统钥到期时停止使用系统钥及产生和使用一新系统钥。

52. 根据权力要求 51 的方法，进一步包括当系统钥到期时保持系统钥以解码之加密的加密钥识别。

53. 根据权力要求 40 的方法，进一步包括使用一有一系统钥共同名称的系统钥加密的加密钥识别，散列系统钥共同名称以产生一系统钥共同名称散列值，及以关联于数据实体地储存系统钥共同名称及系统钥散列值。

54. 根据权力要求 53 的方法进一步包括：

使用一可搜索属性以要求数据操作；

搜索与可搜索属性所相配的；

使用一系统钥散列值搜索系统钥共同名称；

使用一系统钥共同名称搜索系统钥；

以系统钥解码加密钥识别；

使用一加密钥识别搜索加密钥；

以加密钥解码数据实体。

55. 根据权力要求 53 的方法，进一步包括以一个人证书权限确认系统钥，及于系统钥进行一完整性检测。

56. 根据权力要求 40 的方法，进一步包括检测加密钥的期限。

57. 根据权力要求 56 的方法，进一步包括当加密钥期满后产生一新加密钥，使用一加密钥撷取数据实体，以加密钥解码被撷取的数据实体，以新加密钥加密被撷取的数据实体，储存被撷取的数据实体。

58. 根据权力要求 40 的方法，进一步包括散列数据实体的可搜索属性以确定数据实体属性散列值及以关联于数据实体地储存数据实体散列值。

59. 根据权力要求 58 的方法进一步包括：

使用一可搜索属性以要求数据操作；

散列可搜索属性以产生一可搜索属性散列值；

搜索与可搜索属性散列值所相配的；

使用一加密钥识别搜索加密钥；

当撷取加密钥后，以加密钥解码数据实体。

60. 根据权力要求 40 的方法，进一步包括于一传输线上传输数据实体，及当中加密数据实体包括根据一业务法则加密只是一部份的数据实体。

61. 根据权力要求 40 的方法，进一步包括于每一用户对话(session)产生一新的加密钥。

62. 根据权力要求 40 的方法，进一步包括于每一用户行动(action)产生一新的加密钥。

63. 根据权力要求 40 的方法，进一步包括于一独立的数据库撷取加密钥，及以加密钥解码数据实体。

64. 根据权力要求 40 的方法，进一步包括于一要求的事件中审计加密钥。

65. 根据权力要求 40 的方法，当中数据实体及加密钥识别是储存于一第一数据库，及进一步包括储存加密钥于一第二数据库。

66. 根据权力要求 40 的方法，进一步包括以一有系统钥共同名称的系统钥加密加密钥识别，及永远于一保安区域维持系统钥。

67. 根据权力要求 40 的方法进一步包括：

使用一可搜索属性以要求数据操作；

搜索与可搜索属性所相配的；

使用一加密钥识别搜索加密钥；

于系统钥进行一完整性检测；及

以加密钥解码数据实体。

68. 一种于静止时撷取加密数据的方法，此方法包括：

使用一可搜索属性以要求数据操作；

搜索与可搜索属性所相配的一重复数据实体；

于一数据实体中得到一加密钥识别；

使用一加密钥识别搜索加密钥；及

以加密钥解码数据实体。

69. 根据权力要求 68 的方法进一步包括：

于一数据实体中得到一系统钥共同名称；

使用一系统钥共同名称搜索系统钥；

以系统钥解码加密钥识别；

70. 一种储存及撷取加密数据的方法，此方法包括：

以一有一加密钥识别的循环及动态加密钥加密一重复数据实体；
储存该数据实体；及

当一所要求的循环事件发生时产生及循环到一新加密钥。

71. 根据权力要求 70 的方法，当中所要求的事件包括开始一新的用户对话。

72. 根据权力要求 70 的方法，当中所要求的事件包括开始一新的用户行动。

73. 根据权力要求 70 的方法，进一步包括以一有一系统钥共同名称的循环系统钥加密对话加密钥识别。

74. 一种储存及撷取加密数据的方法，此方法包括：

以一有一第一加密钥识别的第一加密钥加密一第一数据实体；
储存该第一数据实体；

以关联于第一数据实体地储存第一加密钥识别；

以一有一第二加密钥识别的第二加密钥加密一第二数据实体；
储存第二数据实体；及

以关联于第二数据实体地储存第二加密钥识别。

75. 根据权力要求 74 的方法，进一步包括以一有一系统钥共同名称的系统钥加密第一及第二加密钥识别，及以关联于第一及第二数据实体地储存系统钥共同名称。

76. 根据权力要求 75 的方法，当中第一及第二数据实体是被联结及相关于一个人的。

77. 根据权力要求 76 的方法，进一步包括：

使用一相关于一个人的可搜索属性以要求数据操作；

搜索与可搜索属性所相配的；

找出相关于一个人的联结第一及第二数据实体；

撷取系统钥共同名称；

使用一系统钥共同名称搜索系统钥；

以系统钥解码第一及第二加密钥识别；

使用第一及第二加密钥识别以搜索第一及第二加密钥；

以第一加密钥解码第一数据实体；及

以第二加密钥解码第二数据实体。

78. 根据权力要求 74 的方法，进一步包括以一有一第一系统钥共同名称的第一系统钥加密第一加密钥识别，及以关联于第一数据实体地储存第一系统钥

共同名称，及以一有一第二系统钥共同名称的第二系统钥加密第二加密钥识别，及以关联于第二数据实体地储存第二系统钥共同名称。

79. 根据权力要求 78 的方法，进一步包括：

使用一相关于一个人的可搜索属性以要求数据操作；

搜索与可搜索属性所相配的；

找出相关于一个人的联结第一及第二数据实体；

撷取第一及第二系统钥共同名称；

使用第一及第二系统钥共同名称以搜索第一及第二系统钥；

以第一系统钥解码第一加密钥识别；

以第二系统钥解码第二加密钥识别；

使用第一及第二加密钥识别以搜索第一及第二加密钥；

以第一加密钥解码第一数据实体；及

以第二加密钥解码第二数据实体。

80. 一电脑系统包括：一加密钥管理员可用以产生一有加密钥识别的加密钥，加密钥可被用以加密一数据实体，及一资料数据库可用以储存于一加密形式的数据实体和资料数据库可被用以关联于数据实体地储存加密钥。

81. 根据权力要求 80 的电脑系统进一步包括一系统钥管理员可用以产生一有系统钥同名称的系统钥，系统钥可被用以加密加密钥识别。

82. 根据权力要求 81 的电脑系统当中资料数据库可进一步用以关联于数据实体地储存系统钥共同名称。

83. 根据权力要求 81 的电脑系统进一步包括一保安令牌及一保安令牌阅读可器用以接收保安令牌，及当中系统钥是被储存于保安令牌。

84. 根据权力要求 83 的电脑系统当中保安令牌包括一灵巧卡及保安令牌阅读器包括一灵巧卡阅读器。

85. 根据权力要求 80 的电脑系统进一步包括一加密钥数据库可用以储存加密钥。

86. 根据权力要求 80 的电脑系统进一步包括一系统钥管理员可用以产生一有系统钥共同名称的系统钥，系统钥管理员可进一步用以散列系统钥共同名称以产生一系统钥共同名称散列值，系统钥可被用以加密加密钥识别，及一系统钥数据库可用以储存系统钥共同名称散列值及系统钥共同名称。

87. 根据权力要求 80 的电脑系统进一步包括一硬件随机号码产生器可用以

产生加密钥。

88. 根据权力要求 80 的电脑系统进一步包括一钥寿命期管理员可用以监察加密钥有效日期及于旧加密钥期满后要求新加密钥。

89. 根据权力要求 88 的电脑系统当中钥寿命期管理员是用以以新加密钥取代加密钥。

90. 根据权力要求 80 的电脑系统当中加密钥管理员是用以当所要求事件发生时产生一新加密钥。

91. 根据权力要求 90 的电脑系统当中所要求事件包括加密钥期满。

92. 根据权力要求 90 的电脑系统当中所要求事件包括开始一新用户行动。

93. 根据权力要求 80 的电脑系统进一步包括一系统钥管理员可用以产生一有系统钥共同名称的系统钥，系统钥可被用以加密加密钥识别，及钥寿命期管理员可用以监察系统钥有效日期及于旧系统钥期满后要求新系统钥。

94. 根据权力要求 80 的电脑系统进一步包括一总保安管理员可用以与外界的电脑系统沟通，当中加密钥管理员只可用以与总保安管理员沟通。

95. 根据权力要求 80 的电脑系统进一步包括一业务逻辑构件 (business logic component) 可用以决定那一部份的数据实体被加密，及当中加密钥管理员不可用以与业务逻辑构件沟通。

96. 一电脑可读媒介包含用以控制一电脑系统作加密及解码数据的指令，借着：

以一有一加密钥识别的加密钥加密一数据实体；

储存该数据实体；

以关联于数据实体地储存加密钥识别。

97. 根据权力要求 96 的方法，进一步包括：

使用一可搜索属性以要求数据操作；

搜索与可搜索属性所相配的；

使用一加密钥识别搜索加密钥；及

以加密钥解码数据实体。

98. 一提供一安全环境以储存资料的方法，此方法包括：

以一有一随机产生的加密钥识别的加密钥加密一数据实体；

储存该数据实体；及

以关联于数据实体地储存加密钥识别。

99. 根据权力要求 96 的方法, 进一步包括以一有一系统钥共同名称的系统钥加密加密钥识别。

100. 一于电脑系统上显示客户资料的方法, 此方法包括:

接收由一用户发出检阅资料的要求;

撷取资料;

检验资料的一保安状况;

评估一保安存取名单以找出一对应于用户的身份;

检验用户的保安存取层次;

基于用户的保安存取层次适配显示参数而改变可用的显示栏(display fields);

基于用户的保安存取层次显示允许的资料及显示栏。

101. 根据权力要求 100 的方法, 当中适配显示参数而改变可用的显示栏包括对应于用户未给与权利检阅的资料以剔除可用的显示栏。

102. 根据权力要求 100 的方法, 当中检验用户的保安存取层次包括检验用户的地位身份。

103. 根据权力要求 100 的方法, 当中检验用户的保安存取层次包括检验用户的用户身份。

104. 根据权力要求 100 的方法, 进一步包括当一负责的用户把资料的保安状况标记为私人时自动加入到保安存取名单上。

105. 一于电脑系统上与一加密伺服器沟通的方法, 此方法包括:

与一加密伺服器的总保安管理员建立沟通;

输入一数据操作的要求;

接收一数据实体以反应该要求;

由数据实体撷取保安钥资料;

要求一加密钥;

接收该加密钥; 及

解码数据实体。

106. 根据权力要求 105 的方法, 当中由数据实体撷取保安钥资料包括撷取一加密钥识别。

107. 根据权力要求 105 的方法, 当中由数据实体撷取保安钥资料包括于一加密表格中撷取加密钥识别及撷取一系统钥共同名称。

108. 根据权力要求 105 的方法，当中由数据实体撷取保安钥资料包括于一加密表格中一加密钥识别及撷取一系统钥共同名称散列值。

109. 根据权力要求 105 的方法，进一步包括接收一重复数据实体以反应要求，由数据实体撷取保安钥资料，要求多重加密钥，及接收多重加密钥。

110. 根据权力要求 105 的方法，进一步包括把一保安令牌插入一保安令牌阅读器。

111. 一作加密及解码数据的加密及解码方法，此方法包括：

以一有一加密钥识别的加密钥加密数据；及

以一有系统钥共同名称的系统钥加密加密钥识别。

112. 根据权力要求 111 的方法，进一步包括以一加密钥管理员数位证书加密加密钥。

113. 根据权力要求 112 的方法，进一步包括以系统钥解码加密钥识别，以一对应于加密钥管理员数位证书的加密钥管理员私人钥解码加密钥，及以加密钥解码数据。

114. 根据权力要求 113 的方法当中在未有授权下解码数据需要至少复制一资料数据库，复制一钥数据库，及复制一证书库。

115. 根据权力要求 111 的方法，进一步包括以系统钥解码加密钥识别及以加密钥解码数据。

116. 根据权力要求 115 的方法当中在未有授权下解码数据需要至少复制一资料数据库，复制一钥数据库，及复制一证书库。

117. 根据权力要求 111 的方法当中解码数据只于运行时间(run time)发生。

118. 根据权力要求 111 的方法当中加密钥是动态和循环的，及系统钥是循环的。

119. 根据权力要求 111 的方法，进一步包括加密系统钥共同名称及储存已被加密的加密钥识别及以关联于以加密钥加密的已加密数据地加密系统钥共同名称。

120. 根据权力要求 111 的方法当中加密系统钥共同名称包括散列系统钥共同名称。

隐藏链路动态钥管理员用于电脑系统有数据库结构作储存加密数据及作储存及撷取加密数据的方法

发明领域

本发明涉及电脑系统数据储存、传输、及撷取/检索的保安。进一步说，本发明涉及用于电脑系统中机密资料的储存、传输、及撷取的加密方法及数据库结构。

发明背景

随着国际互联网及宽频带网络的普及，很多的互联网及电子商贸公司也需要处理于互联网上交换机密资料。机密资料的例子包括信用卡号码、银行帐户号码、社会保障号码、出生日期及高度个人和私人医疗记录。现时以公共密钥结构(PKI)系统发出的电子证书使用安全插座层(SSL)协定以保护转换中的互联网通信。所以，很多的互联网公司是使用防火墙及 SSL 作为保护其客户及其伺服器之间通信的标准方法。

当 SSL 协定由 Netscape Communication Corporation 开发时，它能够提供更 128 位长度的字键，字键越长加密越强。对现今的网络攻击方法而言，这种使用单一及固定的钥密码术而加密机密资料是脆弱的。再者，SSL 只能保护传输中的数据。所以，近来成功地迅速的在不同的网站窃取数以千计的信用卡号码及其他机密资料引起公众的抨击。

一般地，电子商贸公司会把其伺服器存放于设有门锁及监视摄影机的房间以保护其固定的加密钥及敏感的资料。可是，黑客是不需要实质上进入伺服器房来存取储存于公司伺服器上的数据。黑客只需要合法的国际互联网协定(IP)便可进入公司的网络。甚至使用了防火墙，这样的进入也可透过如 IP 欺骗及网络扫描等的入侵方法进行。当黑客进入了网络后，只要使用一般的网络攻击及网络扫描便能取得固定的加密钥。一旦取得了加密钥，黑客便能解密大部分的储存公司伺服器上的资料，当中包括信用卡号码及关于公司员工和客户的其他敏感和机密的资料。

从病人观点来看这问题，未经许可的存取私人病历记录影响更为严重。对一般客户而言，相对于损及名誉和敏感的病历资料被公开的潜在可能时，取消及补发信用卡的不便可算是轻微。再者，非法擅改病历资料是为侵害隐私及可能威胁生命。所以，机密资料的保护，特别是病历记录，需要更大的保证。

新颖的电脑系统使用一隐蔽链路动态钥管理员，那提供加强的加密数据保护。此电脑系统大至上包括一加密钥管理员可用以产生一有加密钥识别的强加密钥。此电脑系统也包括一资料数据库可用以储存一由加密钥所加密的数据实体。此资料数据库可进一步用以储存相关数据实体的加密钥识别。

在最佳的实施例中，此电脑系统也包括一系统钥管理员可用以产生一有一系统钥共同名称的系统钥。此系统钥是用来加密加密钥识别的。所以，加密钥识别最好是在当它被与数据实体相关地被储存时加密。系统钥共同名称也会被与数据实体相关地储存于资料数据库，最好是以散列格式储存。此电脑系统也包括一钥数据库，那是与资料数据库分开的。加密钥及其加密钥识别是储存于钥数据库。最好是，系统钥共同名称是散列于资料数据库，系统钥共同名称散列值是与系统钥共

同名称一同储存于钥数据库。或者，把系统钥共同名称与加密钥识别分开，一分开的系统钥数据库可被提供作系统钥共同名称及系统钥共同名称散列值。系统钥证书，那包括系统钥本身，最好是储存于一保安令牌(token)如灵巧卡(smart card)。所以，本电脑系统提供了一灵巧卡阅读器。系统钥证书也是储存于此灵巧卡。

本电脑系统也包括一钥寿命期管理员可用以管理加密钥的有效期及当旧的加密钥期满后要求新的加密钥。在一实施例中，此加密钥最好是动态的及经常转换。当要求转换事件发生时，例如当用户开始一新的工作，加密钥便转变或转换。加密钥是动态的，当加密钥期满后，本电脑系统会撷取所有以旧加密钥加密的数据及以新的加密钥加密数据。系统钥最好是转换而不是动态的。加密钥管理员是储存于保护区域，电脑系统会使用一总保护管理员作为一保护区域的闸门管理者。要加强保护，加密钥管理员可只是与总保护管理员通讯。

于一替代的实施例中，钥寿命期管理员可用以旗标期满的钥及转变或停止期满的钥于下一用户要求或联络时。在本实施例中，当数据被撷取后，期满的加密钥被取替，加密钥是动态的。在本实施例的一个优点是钥寿命期管理员不会控制资料数据库的存取从而减低钥寿命期管理员被未经授权而存取的机会。

本发明的另一特色是，一种根据本发明而作储存及撷取加密资料的方法是以本发明的电脑系统而实施。综合地说，此方法包括以一有加密钥识别的加密钥加密数据实体。数据实体会被储存，而加密钥识别以相关于数据实体地被储存。

在最佳的实施例中，用户使用一可搜索的属性(如一客户名称)以要求数据操作(如检阅、更新、或加入资料)。一搜索查询被发出作相配可搜索的属性。较佳地，

可搜索的属性是散列以减少搜索时间及增加保安。当相配被找出后，保安钥资料会被于数据实体中取出。保安钥资料最好包括在一加密表格中的加密钥识别及系统钥共同名称散列值。之后，使用系统钥共同名称散列值设置系统钥共同名称，及系统钥共同名称会被用以撷取系统钥。较佳地，一私人证书机构查证系统钥数字证书。系统钥之后会被用作解码加密钥识别，那会依次被用作设置加密钥。数据实体之后会以加密钥解码。因为加密钥的循环特性，多个的加密钥可能会被用作加密与一个人相关的资料。再者，因为系统钥的循环特性，不同的系统钥可能会被用作加密与一个人相关的加密钥识别。因为系统钥是储存于灵巧卡或其他保安令牌，那是储存于保安区域中，系统钥永远不会离开该保安区域，及假如系统钥共同名称是如理想地被散列系统钥共同名称永远不会离开该保安区域。

于本发明的另一特色，于电脑系统中提供一电脑可读媒介于静止原状加密数据。电脑可读媒介包含一作储存加密数据的数据库结构。数据库结构包括至少一以至少一加密钥加密的数据实体及至少一相关于数据实体的加密钥识别。

在一最佳的实施例中，系统钥是用作以其公共钥加密加密钥识别，及数据库结构进一步包括系统钥共同名称散列值。最佳地，数据库结构包括两个数据库，资料数据库，那包含数据实体，及一钥数据库，那包含加密钥，加密钥识别，系统钥共同名称散列值，及系统钥共同名称。在另一实施例中，一系统钥数据库可被提供，那储存系统钥共同名称及系统钥共同名称散列值。如前文所述，一重复数据实体最好是以一重复的加密钥加密，及加密钥的加密钥识别是以多重的系统钥加密。数据库结构进一步包括保安令牌，最好是一灵巧卡，那储存系统钥的数字证书及加密钥的数字证书。

于本发明的进一步特色，根据本发明的一电脑可读传送媒介包含所述数据结构。

在一最佳的实施例中，数据传送媒介包括用作与保安区域中的总保护管理员和在其他区域中的资料数据库沟通的 IPSEC 安全频道。

于本发明的再进一步特色，一提供一安全环境作储存资料的方法是实施于本电脑系统中。方法包括以一加密钥加密数据实体，及储存该数据实体。加密钥识别以相关于数据实体地被储存。最佳地，一有系统钥共同名称的系统钥会被用作加密加密钥识别。

于本发明的另一特色，一于电脑系统上显示客户资料的方法。大致地，一已确实或信任的用户输入检阅资料的要求，那之后被撷取。电脑系统之后会检验资料的保安状况，及评估一保安存取名单以找出一对应于用户的身份。检验用户的保安存取层次，及基于用户的保安存取层次适配显示参数而改变可用的显示栏。之后显示允许的资料。

在一最佳的实施例中，适配显示参数包括对应于用户未给与权利检阅的资料以剔除可用的显示栏。用户的身份可被指明用户的特性，或用户的保安层次或地位。再者，当一负责的用户把资料标记为私人时，负责的用户会被自动加入到保安存取名单(SAL)上。保安存取名单也会控制那用户可以修改资料及那用户只可检阅资料。

于本发明的另一特色，一实施于电脑系统上作为与加密伺服器沟通的方法。本方法包括与一加密伺服器的总保安管理员建立信任的沟通，及输入一数据操作的要求。接收一数据实体以反应该要求及由数据实体撷取保安钥资料。保安钥资料是用作要求一加密钥，及接收该加密钥后，数据实体会被解码。

在一最佳的实施例中，撷取保安钥资料包括于一加密表格及一系统钥共同名称散列值中撷取加密钥识别。此外，一般地，一重复数据实体会被提供以反应要求，及源自数据实体的保安钥资料包括重加密钥及多重系统钥共同名称散列值。因此，多重加密钥会被要求，及多重加密钥会被接收以解码重复数据实体。

因此，本发明的目标是提供一用于储存加密数据的数据库结构的电脑系统的改良系统及用作储存及撷取加密数据的方法。

附图简述

图 1 是一根据本发明的一实施一隐藏链路动态钥管理员的电脑系统的原理图；

图 2 是一图 1 的电脑系统的原理图方块图，说明电脑系统的软件构件；

图 3 是根据本发明及由图 1 的电脑系统所使用的数据库结构的原理图；

图 4 是一图 4 的数据库结构的保安钥识别属性的原理图；

图 5 是一监视器的原理图，说明根据本发明的能适应的显示参数及只有公共资料和栏可被显示；

图 6 是一监视器的原理图，说明根据本发明的能适应的显示参数及公共和私人资料和栏可被显示；

图 7 是一原理图方块图，说明决定如何适应说明于图 5 及图 6 的显示参数的步骤；

图 8 是一时段(session)加密钥数据实体的原理图；

图 9 是一系统钥共同名称数据实体的原理图；

图 10 是一原理图方块图，说明当一加事务处理时数据实体的加密及储存；

图 11 是一原理图方块图，说明当更新及浏览事务处理时数据实体的撷取及解码；

图 12 是一原理图方块图，说明当更新及浏览事务处理时数据实体的撷取及解码的另一实施例；

图 13 是一原理图方块图，说明去活(deactivation)时段加密钥；及

图 14 是一原理图方块图，说明说明去活(deactivation)时段加密钥的另一实施例。

发明内容

参照附图，图 1 及 2 显示一电脑系统 20 说明根据本发明的最佳实施例而构成，用作储存资料。本发明提供一于静止时加密及解码数据的改良方法。电脑系统 20 大至上包括一有加密钥管理员(EKM)24，系统钥管理员(SKM)84，钥寿命管理员(KLM)88，钥审查管理员(KAM)90 及数据库适配器(DBAD)86。电脑系统 20 也包括一有一资料数据库的重复的用户商业区域 26。电脑系统 20 根据本发明实施一方法。该方法大至上包括如说明于流程图图 10 解码及储存数据实体 30(图 3)，及该方法也包括撷取及解码数据作数据操作。一撷取及解码方法的实施例说明于流程图图 11。电脑系统 20 使用一说明于图 3 的数据结构。数据结构大至上

包括一有保安钥识别属性 32 的重复数据实体 30，那包含保安钥资料如说明于图 4。

参照图 1，除了保安区域 22 及用户商业区域 26 外，电脑系统也包括重复用

户终端机 34。用户终端机有通讯能力以能与商业区域 26 沟通，最佳是透过国际互联网 36 使用 PKI 及 SSL 以提供用户终端机 34 及商业区域 26 之间的通讯保安。本发明也打算使用如内联网，区域性网络(LAN)，及宽域性网络等的专用通讯线。内联网，LAN 及 WAN 应用可被使用于任何机构，当数据保安是重要时，例如：银行，医院或律师行等。用户终端机 34 只能透过保安协定(如：防火墙)才可进入用户商业区域 26。用户商业区域 26 及保安区域 22 之间的通讯最佳是透过因特网协议安全层，虚拟专用网隧道 38(IPSEC, VPN tunnel)进行。

保安区域 22 包括一主钥伺服器 40，一次钥伺服器 42，一保安钥数据库(KEYDB)44，及一证书权限伺服器 46。每一钥伺服器是有数个的方便构件包括小型电脑系统接口(SCSI)卡，保安硬件配接器，双 700MHz 处理器及反射式 20GB 硬盘。证书伺服器 46 也包括数个的方便构件，包括小型电脑系统接口(SCSI)卡，单 700MHz 处理器及反射式 30GB 硬盘。最佳地，保安区域构件之间能进行构件互相验证。COM+，CORBA 或 Java 保安可用作控制互相验证。

主钥伺服器 40 及次钥伺服器 42 是反射式构件。所以，主钥伺服器及次钥伺服器是相当的相似。当主钥伺服器故障时，次钥伺服器可立即运作而不会影响系统操作，因此提供很好的容错。主及次钥伺服器 40，42 之间的操作的移转是以一心跳容错移转(heart beat failover)通道而实行。每一主及次钥伺服器 40，42 包括一磁带备用 48，50，当 KEYDB44 不能恢复或钥完整性失败时用以撷取钥。主伺

服务器 40 有一主系统钥阅读器 52，命名为阅读器#1 于附图，及一主加密钥阅读器 54，命名为阅读器#2 于附图。最佳地，主伺服器 40 的每一主阅读器 52，54 也储存相同资料。所以，主阅读器 52，54 是反射式硬体构件以提供很好的容错。次阅数据库 42 也包括一次系统钥阅读器 56，命名为阅读器#1 于附图，及一次加密钥阅读器，命名为阅读器#2 于附图。最佳地，次伺服器 42 的每一次阅读器 56，58 也储存相同资料。所以，次阅读器 56，58 也是反射式，及总共有四个阅读器可撷取钥资料。阅读器 52-58 包括保安令牌阅读器作接收保安令牌。最佳地，阅读器包括灵巧卡阅读器作接收灵巧卡。一硬件随机号码产生器(HRNG)59 可用以于保安区域产生随机号码，那是用作钥的识别码。当一软体随机号码产生器 HRNG 59 可能被用时，HRNG 59 最好增加其速度。

KEYDB 44 包括一有一容错系统的外置硬盘阵列以反射式操作提供很好的容错。外置硬盘阵列包括一磁盘机的冗余式阵列(RAID)最好是有五个硬盘。KEYDB

最好是以 RAID 第 5 级操作，那提供于字节级的数据带状处理法及带错误改正资料。每一钥伺服器 40, 42 透过 IP 与 KEYDB 44 通讯及使用如前文所述的互相验证。

用户商业区域 26 最好包括一重复用户伺服器 60, 61 及一资料数据库 62, 那是与 KEYDB 44 分离的。最佳地, 一备份资料数据库 64 也会被提供。备份资料数据库 64 反射主资料数据库 62 以提供备份及保护数据损耗。所以用户商业区域 26 是有很好的容错。为增加保安, 用户商业区域伺服器 60, 61 只可透过防火墙 66 接入。每一用户伺服器 60, 61 可包含多个商业逻辑构件, 例如: 第一号商业逻辑构件 (BLC1) 68。BLC 包含由用户所设定的指令及规则以操作电脑系统 20。

所以, BLC 提供权力给用户以决定某一些系统操作选项。

一般地, 每一终端机 34 包括一中央处理器 (CPU) 70, 一数据输入装置 (如: 键盘 72) 及一显示器 74。CPU 70 是作为控制显示器 74, 由键盘 72 接收输入, 及使用一调制解调器, 双向卫星, SDL 或其他通讯器材建立和维持透过国际互联网 36 沟通。CPU 70 也可控制其他电脑系统装置 (如: 打印机或磁盘机)。在一最佳的实施例中, 保安令牌阅读器 78 包括一灵巧卡阅读器以接收灵巧卡 80。灵巧卡阅读器 78 是一私人及安全档案系统。每一用户是有他们自己的灵巧卡 80, 那包括一用作识别及确实用户的用户数字证书。其他已知的方案, 如用户确实及密码可用作控制存取及确实用户。身份识别可包括辅助级别, 招待级别, 行政级别, 及其他。身份识别代表个人于其级别的责任及其责任所需要资料的范围。用户及身份识别可如以下及相连至图 7 地使用以限制资料的存取。

参照图 2, 电脑系统 20 的保安区域 22 包括数个软体构件, 那是存在于硬体构件 (说明于图 7)。主及次钥伺服器 40, 42 包括大至上相同的软体构件, 两者也会 (参照主钥伺服器 40) 地被描述。主钥伺服器 40 包括数个软体构件: 一总保安管理员 (GSM) 82, 一加密钥管理员 (EKM) 24, 一系统钥管理员 (SKM) 84, 一数据库适配器 (DBAD) 86 及一钥审查管理员 (KAM) 90。一证书管理员 (CM) 92 会于私人证书机构 (CA) 伺服器 46 内被提供。

总保安管理员 (GSM) 82 是作为位于保安区域 22 的电脑系统 20 部分的网关。在那方面, 保安区域 22 的每一构件 EKM 24, SKM 84, DBAD 86, KLM 88, KAM 90, CM 92 最好不能与其他在电脑系统 20 的保安区域 22 以外的构件直接沟通。他们只能透过 GSM 82 与外界沟通。最佳地, 构件与 GSM 82 互相验证, 那是位

于保安区域及在商业区域构件 68 以外。COM+, CORBA 或 Java 保安可用作控制互相验证。所以, 透过信任认证处理, 用户或任何构件也不能透过 GSM 82 以外的与其他接触。

GSM 82 也可用作加密数据实体 30(图 3), 以由 BLC's 及电脑系统 20 的其他部件所要求和指挥, 使用一三重数据加密标准(3DES), RC4, 或任何强力对称密码算法于数据实体 30C, 30D 的选定属性。所以, 当 DES 使用对称 64-bit 钥作加密, GSM 使用 3DES 或对称 192-bit 钥作加密。使用这些延伸长度使钥更难解破。GSM 82 也用作解码数据实体 30, 当其他电脑系统 20 的部件要求解码时。进一步, GSM 82 也可用作进行散列, 以报文分类算法(MD5), SHA-1 或其他强力散列算法, 如由其他部件所指示。散列值或完整值于一单向散列处理多数会以属性储存于数据实体作完整性检验用途。最佳地, GSM 82 散列所有数据实体的数据属性及以一属性储存这些数据散列值。当数据被解码后, 它会再被散列及比较之前和之后的散列值。假如两个散列值是相同的话, 于数据实体的数据完整性便会被确定。假如两个散列值是不相的话, 一警报便会被发出及数据会由备份资料数据库 64 中撷取。

加密钥管理员(EKM)24, 如其名称, 主要是管理加密钥, 如以下所述是用作密钥及解码数据实体 30C, 30D。所以, EKM 24 是可使用 3DES 或 RC4 来产生多个加密钥(SEK)及产生给 SEK 的时段加密钥识别(SEKID's)。SEKID's 是一随机号码, 最好是由 HRNG 59(硬件随机号码产生器所)产生。因为 SEK 是动态和循环的, 会于以下详细说明, 他们被认为是时段加密钥因为一新的 SEK 会被产生, 至少于每一个新用户时段或在该时段中要求。所以, EKM 24 是可用以指示电脑系统去改变或循环 SEK, 当一循环事件发生时, 例如开始一个新用户时段。最佳地, 新的 SEK 会被产生得更频繁, 如以下所述, 所以 SEK 是更适当及通常会被认为是加密钥。EKM 会被用于 SEK 以 SEK 的散列值进行完整性检验。EKM 进一步可用作传送 SEKID 到 SKM84 作加密, 及 EKM24 也可用作传送 SEK 及对应 SEKID, 于加密形式, 到 GSM82, 之后以 SEK 加密数据实体 30C, 30D。

系统钥管理员(SKM)84 主要是管理系统钥, 如以下所述, 是用作加密 SEKID。所以, SKM 84 是用作以强力加密法产生系统钥。最佳地, SKM 产生强力 PKI 1024-bit 钥作系统钥。所以, 系统钥最好是使用不对称加密, 那每一系统钥便有一公共钥及一私人钥。SKM 也产生一系统钥共同名称(SKCN)给每一系统钥。SKCN 会被产生当产生系统钥的 PKI 数字证书时, 所以每一系统钥有其不同的

SKCN。SKM 也会由 EKM 24 接收 SEKID 及以公共钥加密 SEKID。当 EKM 24 要求时，SKM 84 也会以私人钥解码 SEKID。如有需要，SKM 84 及 EKM 24 可合为一构件及可存在同一伺服器或处理器中。

在一最佳的实施例中，使用 Microsoft Crypto API (应用程序接口)，GSM82 也会以一 EKM 内置数字证书公共钥加密 SEK 及以一 EKM 内置证书私人钥解码 SEK。EKM 内置数字证书是储存于一证书储存器，最好是主加密钥阅读器 54。系统钥数字证书也是储存于一证书储存器，最好是主系统钥阅读器 52。因为私人证书机构的证实要求，系统钥及 EKM 在保安区域 22 外是废弃不用的。这也要求如下描述的解码方法，当电脑系统操作时。那是当系统运行时间。

钥寿命管理员 (KLM) 88 监视 SEK 及系统钥的寿命，基于它们的有效日期及时间印章。最佳地，KLM 88 以一期限旗标旗标到期的 SEK，当在下一个要求时，KLM 便会检查 SEK 的期限状况及在运行时间时以新钥的取代到期的 SEK。或者，KLM 88 去活到期的 SEK 及产生取代 SEK。要立即去活到期的 SEK，所有由 SEK 加密的数据会被撷取及以新 SEK 加密。立即去活 SEK 要求 KLM 88 控制资料数据库 62 的存取。所以，运行时间或“呼叫”去活会较佳。KLM 88 也指示电脑系统产生新的系统钥。但是，因为 SEKID 的数目是电脑系统钥加密，系统钥最好不去活。

(KAM) 90 是用作维持一定活动审计记录，包括所有有关 SEK 系统钥的处理，一般地，KAM 90 监控警报事件记录，使用智能模式，规则及政策。KAM 90 也是可用作提供通知，当一警报事件发生及假如一系统钥或 SEK 不协调时，KAM 90 是用作指示 EKM 24 或 SKM 84 更改和/或去活 SEK 或系统钥。

证书管理员 (CM) 92 是用作进行所有有关系统钥 PKI 的操作。CM 92 为每一系统钥产生一 X.509 数字证书。最佳是，数字证书包括一重覆 V3 外延，所以只有私人证书机构 (CA) 可查证该钥。每当 SKM84 接收到要求系统钥解码时，CM 会与 CA 沟通，那是置于保安区域，以查证系统钥。

DBAD 86 是用作隐藏数据库指定的 API，于保安区域 22 构件的从而控制及加强钥管理员 24, 84 及保安钥数据库 44 之间的沟通。所以，以使用不同的 DBAD，保安区域构件可与不同类的数据库接口。一最佳的数据库是一 VERSANT 面向目标数据库管理系统有一内建容错，伸缩性，目标水平锁定，一目标加速器，平行询问引擎，及其它特色。DBAD86 也容许保安区域构件与多个于保安区域 22 的数据库接口，如 Microsoft SQL Server, Sybase, Informix, Oracle, 及

IBM DB2。所以，DBAD86 是可用作当主数据库失校时转换备份数据库而没有迟延。

参考图 3，数据库结构最好是包括有一重复数据库实体的 30 面向目标数据库，那是一数据物件。但其它的数据库也可用于本发明上，例如：关系数据库，如 Microsoft SQL Server, Oracle, Sybase, Informix 及 IBM DB2。所以当术语“object”可被使用时，“record”也可被使用。

其中一数据库实体 30A，特别的一持续数据实体，是详细地被显示。数据库实体 30A 包括一加入 (added) 100 及一谁加入 (Added By) 属性 102。加入属性 100 记录

一时间印章包括日期及时间，当物件加入时，及谁加入属性 102 记录用户的数字签名，当用户加入记录或数据实体时。数字签名是从用户灵巧卡 80 的数字书或用户现时的时段和用户身份中得到。更改 (Modified) 及谁更改 (Modified By) 属性，集成 104，记录相同资料作更改到数据实体 30A。这些非拒绝属性 100, 102, 104 阻止一用户宣称一些动作不是由该用户作出的。保安状况 (Set Status) 属性 108 指出那数据物件含有文字或密码文字及那是公共或私人。

再参考图 4，一保安钥识别属性 32 也是一数据实体 30A 的属性及包含保安钥资料。保安钥资料包括加密 SEKID112 及 SKCN 散列值 114，是用作找出相关的加密数据实体 30C, 30D 及找出用作加密 SEKID112 的系统钥。SKCN 散列值最好是储存于保安钥属性 32，SKCN 可没有散列地被储存于这位置。

再参考图 3，数据实体 30A 也包括一保安完整性属性 (SecIntegrity) 116，那包含数据实体散列值。数据实体散列值是由散列于数据实体的所有或选择属性所得到。这是由商业需要及政策所控制的，最好是由用户及 BLC 中的记录所决定。当一数据实体被撷取后，会以 MD5 散列及把数据实体散列值与存于保安完整性属性 116 的散列值作比较。如果散列值是相同，完整性便被确定正确及不会更改。如果散列值是不同，警报便会发出，数据可被人手确定，由备份资料数据库 62 中撷取。

再参考图 5, 6 及 7，一保安私隐属性 118 控制于相关数据实体 30C, 30D 中的资料的存取。当一用户，如一医生，标记他的资料是私人时，一特别存取表 (SAL)，数据实体/类别 30B 是自动产生及医生是自动加到 SAL。医生由 SAL 可加入或删除用户识别属性 120 和/或地位识别 122。用户属性 120 是基于由灵巧

卡或其他验证方法指定用户识别。地位识别 122 是基于用户的不同保安级别。例如，医生可许可其他医生检阅私人资料但护士便不可。地位可包括任何保安级别，例如：秘

书，股东，守却，及行政等。医生可控制谁能检阅那些资料及谁可更改甚么资料。相同地用于病人记录，当中医生及护士可完全存取，文员是能有限地存取。这些私稳可被用于其它方面如银行，知识产权系统，电子商业，律师行等。

当验证用户要求资料步骤 124(图 7)，电脑系统于步骤 126 撷取资料。当资料被撷取后，系统查证保安私稳属性 118 于步骤 128。如果资料不是标记为私人，它会全被显示于显示器 130(图 6)。如资料是标记为私人，系统检查用户的保安级别于步骤 132。当用户保安级别检查时，系统会检查用户识别及地位识别是否在 SAL，及决定用户有的资料权限。如用户是没有检阅私人资料的权限，显示参数会被更改于步骤 134。于步骤 134，私人资料的显示档不会被显示。

进一步，试想像，公共资料档可被更改，所以私人资料的现是被完全遮盖。于例子中，私人资料 138，如出生日期及孩子数目是显示给有存取私人资料权的用户。但是，在一没有授权检阅私人资料的用户时，出生日期及孩子数目档会被在图 5 的显示中除去。进一步，住址资料 140 及工作地址资料 142 会被显示给有检阅私人资料权限的用户。相反，对于没有存取私人资料权限的用户，除了不能看到住址，工作地址外，档 144(图 5)被更改以不能识别这是一工作地址。

再参考图 3，持续的数据实体 30A 也包括数个相关的属性，那是被数据律规划所使用以联系有关的数据实体 30B, 30C, 30D 到持续数据实体 30A。持续物件 30A 包括一类别识别属性 146 及最少两个找寻属性 148。作更为及更安全的找寻，可找寻属性 148 最好是用户资料的散列值，如病人名称。数据库使用这些属性 146, 148 及其它以联系有关的持续物件 30A 及有关的类别物件 30B, 30C, 30D 与持续物件包含保安钥识别 32，那是用作加密于类别物件的数据属性。两个示范的类别物件(图 3)：一个人类别物件 30C 及一名称类别物件 30D。其他没有说明的

类别物件/实体包括一地址，雇主，缴费，保险及其他。

数据库也提供有一查寻图(look op maps)或笔记 150。所说明的查寻图 150

是作个人类别的性别。这节省数据库资源，因为每一个人于数据库中也简单地以 0, 1, 或 2 对应不明，男或女。所以查寻图 150 节省数据库资源，因为每一个人只有一单数字而不入是一长文字。查寻图也是较佳地用作保安状况属性 108，保安私稳属性 118 及其它。

参考图 8 及 9，数据结构包括一 SEK 物件 151 储存于 KEKDB44 及一 SKCN 物件 152，那是储存于 KEKDB44 或于另一实施例中，一分离系统钥数据库(没有被展示)。所以，为要增加保安，几个的数剧实体是被储存于分离的数据。SEK 物件/实体包括 SEKID153 属性于正常/解玛形式，SEK154，SEK 完整性检测 155，那是 SEK 的散列值，及 SKCN 散列值 156。SEK 数据实体 151 最好是不包括加密的 SEKID。这产生在加密数据及用作加密它的 SEK 一稳藏连路，因为 SEKID 是加密的，及 SEK 是储存于一分离数据库。SEK 也包括一产生于(Created On)厉性 159，那记录 SEK 产生的一时间印章及一最后使用日期属性 161，那记录 SEK 最后一次使用的时间印章。再者，SEK 物件最好是有一使用计数器属性 163，那记录 SEK 被使用过的次数。产生于 159，最后使用日期 161，及使用计数器 163 属性提供用户选择功能。用户可选择使钥在产生后一定的月份期满，例如：两个月。用户也可一定当钥没有于一段时间内被使用或当他们被使用超过某时间时期满。用户也可选择使 SEK 随机地期满。SKCN 物件/实体包括 SKCN 散列值 157 及 SKCN 属性 158，及最好是储存于一与数据实体 30 分离数据库。

以上描述的电脑系统及数据库构是用于加密，储存，撷取及解码数据的方法。当一用户要求一数据操作时，包括加入，更新，检阅，电脑系统便会实施适当的步骤。对于每一交易这是假设用户使用一信任的查证方法；例如灵巧卡或两个素(two factor)查证装置得到商业区域的存取权。

图 10，第一步 160 在加入交易是由用户输入数据到用户的浏览器中。于步骤 162，输入的数据后被传送到 BLC68 给用户。BLC68 之后于步骤 164 要求 GSM82 根据由用户所设的商业规则加密数据。商业规则可由用户更改，会决定那些数据的属性会被加密。GSM82 之后会要求 EKM24 产生一 SEK 于步骤 166。于步骤 166，EKM 产生 SEK 及 HRNG59 产生 SEKID。EKM 之后要求 SKM84 以一系统钥加密 SEKID。SKM84 得到现时的系统钥及由保安区域的 SKCN，系统灵巧卡阅读器 52 及卡于步骤 168。SKM84 之后加密 SEKID 于步骤 170。本方法最好是使用 SEKID 的对称加密，SEKID 最好是以系统钥的公共钥加密于步骤 170 及回到 EKM24。GSM82 之后散列 SKCN 及 SEK 以得到各个的散列值于步骤 172。SKCN 及 SKCN 散

列值之后被储存于 SKCN 数据实体于步骤 174。之后，于步骤 176，SEK，SEKID，SKCN 散列值及 SEK 散列值被储存如 SEK 数据实体 ISI 的属性，于 KEYDB44。GSM82 之后根据 BLC68 的商业规则以 SEK 加密数据实体 30C，30D 于步骤 178，SEK 会被于记忆体中销毁于步骤 180。步骤 182，被加密数据实体 30C，30D 及其相关的持续数据实体 30A 会被对应用户 BLC68 地储存在资料数据库 62。资料也会被储存于备份资料数据库 64。操作是同时于系统的反射构件中进行，资料可于反射构件中撷取，当主构件失效时，所以这里不会进一步谈论反射构件的操作。加密 SEKID12 及 SKCN 散列值 114 是储存于持续数据实体 30A 的保安钥识别属性 32。

参考图 11，于步骤 184 更新及检阅数据操作的种类要求是由用户要求数据操作开始，基于可找寻资料如客户名称。可找寻资料是放步骤 186 中被散列，及一找寻询问在步骤 188 被发出到料数据库 62 以出于可找寻属性 148 中散列值相配的持续物件/实体。相配的持续物件 30A 会于步骤 190 回到相关的数据类别 30C，30D，保安钥资料包括 SKCN 散列值 114 及加密 SEKID112 会从持续实体 30A 的保安钥识别属性 32 中得到。BLC66 之后会透过 GSM82 送出一解码要求到保安区域 22。GSM82 会由数据实体中抽取加密了的 SEKID112。一找寻询问 192 会使用 SKCN 散列值发出到 KEYDB44 以由 KEYDB 取得 SKCN。以 SKCN，于步骤 192 可由保安区域灵巧卡阅读器及卡得到私人系统钥。步骤 196，SKM84 及 CM92 确定系统钥的数字证书。步骤 198，SEKID 以适合的系统钥解码。一找寻询问一会使用解码了的 SEKID 再一次发出以取得 SEK。

于步骤 202，SEK 之后会被散列，散列值会与由持续 SEK 物件 151 的保安完整性属性 155 所得的散列值作比较。如果散列值是相同的话，正确的 SEK 便会得到作解码，及于步骤 204GSM 以 SEK 解码数据实体 30C，30D。假如散列值是不同的，警报便会发出表示钥已损坏。当 SEK 损坏了，而要解码数据实体，正确的 SEK 便要从主备份磁带中取得。从备份磁带取得的 SEK 会被散列，散列值会再与保安完整属性比较以确定 SEK 的完整性。如有需要，SEK 可从次备份磁带 50 中取得。最后，解码数据实体会透过 IPSEC VPN 通道传送到商业区域 BLC 66，之后使用 PKI 到用户终端机 34。图 12 说明另一实施例作更新及检阅数据操作。首三个步骤，传输要求 208，散列可找寻资料 210，及于持续物件 212 中找寻配合散列值，是与之前的实施例(图 11)一样。于图 12 的实施例中，撷取数据是传送到用户终端机(步骤 214)。用户 CPU70 由持续实体 30A 取得保安

钥资料(步骤 216)。于步骤 218, SKCN 散及加密 SEKID 是被传送回 GSM82。SKM 找寻配合 SKCN 散列值(于步骤 220)及取得一私人系统钥(于步骤 222)。以私人系统钥解码 SEKID (于步骤 224), SEK 被取得(于步骤 226)。于本实施例, SEK 之后会以 128-bit SSL 或 IPSEC VPN 被传送到用户终端机(于步骤 228)。如需要, SEK 可被完整性检测, 用户 CPU 用 SEK 解码之前传送的加密数据实体(于步骤 230)。

如上述所示, SEK 最好是动态及循环的。SEK 是循环, 当一循环事件发生 SEK 便会更新。一循环事件是开始一新用户时段。但是, 循环事件最好是通常发生。例如: 一新 SEK 会被要求, 每当用户输入一要求或每次用户转换数据挡。所以, SEK 是时常循环的, 一客户或病人资料会被多个的 SEK 加密。再者, 当个人客户资料更新, SEK 可能与该资料第一次输入时不同, 使到同一客户的资料由不同的 SEK 加密。系统钥也会循环, 但最好是较少次数。因此, 不同的 SEKID 阙系到一个人客户的资料是由不同系统钥加密。

SEK 也可是动态的, 所以当 SEK 期满后, 如图 13 所示的去活及取代。KLM88 检测 SEK 期限(于步骤 232), 假如 SEK 于步骤 234 没有期满, KLM 会继续检测。当 KLM88 找到期满的 SEK, KLM 会要求 EKM24 产生一新的 SEK(于步骤 236), EKM24 也侠 HRNG59 产生一新的 SEKID 作新的 SEK。于步骤 238, EKM 设定一期限给新的 SEK。于步骤 240, SEK 物件 151 给期满的 SEK 是由 SKD44 使用期满的 SEK 的 SEKID 所撷取。SKCN 使用储存于 SKCN 散列值所取得(步骤 242)。接漂, 公共系统钥可由保安区域灵巧卡阅读器 52 所取得(步骤 244)。一询问之后被发出到资料数据库 62 作配合 SEKID 加密值。使用旧 SEK 的数据会被撷取及解码(步骤 248)。数据会以新 SEK 被加密(步骤 250), 数据会被储存(步骤 252), 包括新保安钥识别 32。假如 KAM90 发出一警报及一用户指示系统去话 SEK, 相同的程序发生。由于大量的 SEKID 是由一单一系统钥所加密, 系统钥最好不是动态的。系统钥最好不是时常循环。但是, 于低可能性的情况下, 系统钥会被去活。

图 14 是另一实施例, KLM 也检测 SEK 是否期满(步骤 260)。可是于步骤 262, 当 KLM 找到一期满的 SEK, KLM 在 KEYDB44 中标记 SEK 是期满的。在下一个客户要求(步骤 264), 数据会根据要求地被撷取, 之后于步骤 266, SEK 会被

检测, 看看是否期满。假如 SEK 不是期满, 电脑系统 20 会继续如前文所述。如 SEK 是期满, EKM 会以一新的取代(步骤 268)。再进一步, 于这实施例中, SEK 是动态的, 当数据提出它会被去活, 此与之前图 13 的实施例相反。所以,

图 13 是实施例使用立即及同时去活，图 14 是实施例使用提出去活。系统钥不能被去活，除非新 SEKID 被使用。所以，当一 SEK 被去活后及新 SEKID 必须被加密作储存于保安钥识别属性 32，之后现时的系统钥会被用作加密新的 SEKID。所以，不常循环的系统钥最好不是动态。

电脑系统 20，数据库结构，及根据本发明的方法提供一资料储存及撷取是较之前的加密概念为佳。作为一个人解码一单一客户资料，黑客(hacker)要穿过 GSM82 以取得存取保安区域。之后，黑客要找寻一穿过 IPSEC 通道的方法以存取资料数据库 62。黑客要追踪所有有关的以找出持续数据实体 30A 及关连数据实体 30B, 30C。黑客之后再要检测每一数据实体是否被加密。黑客要找出保安钥识别属性 32 及取出加密 SEKID 及散列 SKCN。黑客之后再要取得安全钥数据库的存取权，及找出保安系统钥共同名称。再者，可能有多于一个的保安系统钥共同名称散列值，所以黑客必需得到多于一个的保安系统钥共同名称。当得到保安系统钥共同名称后，黑客要到保安区域灵巧卡阅读器以得到系统钥。系统钥之后会被一私人证书机构认证。假如黑客能完成以上的步骤，黑客要用系统钥解码适当的 SEKID 于每一数据实体使用认证及有关的系统钥。黑客要通过于保安区域的 KEKDB 44 以取得基于 SEKID 的 SEK。于保安区域设置保安协定，完成所有这些工作而没有被发现是不可能的。假如黑客多次直接尝试破解钥，他是不会成功。因为，本电脑系统及方法使用 3DES 或 RC4 加密，这使黑客需要更长时间来破解一 SEK，因为一单一病人记录会被多个 SEK 加密，黑客可能要花一生时间来得到一病人记录。令破解工作更难的是需要破解一 1024-bit 系统钥。所有破解的工作要在不被 KAM 90 或闯入探测软体发现下进行。

如果黑客尝试下载数据库 62 及破解 SEK，黑客要破解很多 SEK 以取得一单一客户记录，因为黑客是不知那数据实体是关于该客户，黑客要破解数百个 SEK 以取得一单一客户记录。要取得所有客户记录，黑客要破解数百万的 SEK。如果黑客尝试及成功下载于保安区域设 22 的 KEYDB 44，黑客要破解更强的不对称系统钥以解码 SEKID。如果 Microsoft Crypto API 是被使用，黑客要破解 EKM 证书不对称钥，那也最好是 1024-bit 钥。要避免破解系统及 EKM 钥，黑客要偷取证书储存。因为系统及 EKM 钥只能够于灵巧卡阅读器 52, 54 中找到(它们会于使用完毕后被从所有记忆体中删除，如 RAM)。黑客须需要实质的存取灵巧卡阅读器 52, 54 及重建保安区域 22 和模拟系统运行时间。

所以，一隐藏链路动态钥管理员用于电脑系统有数据库结构作储存加密数

据及作储存及撷取加密数据的方法是被透露，那使用由系统钥加密的一加密钥识别及一关联于加密数据的散列统论共同名称以阻止未授权的数存取，以提供更安全的加密数据。虽然说明书已说明及述了本发明的各种不同的具体实施例，但是对本领域的技术人员来说，将会出现多种改型及变换。在不脱离由所附的权利要求书限定的本发明的的精神及范围下，这样一些改型及变换是可以预料并可做到的。例如：不同种类及形式的数据库可被使用，及本发明可应用到被传送的数据。再者，被透露的加密系统应用是作病人记录。因为他们的敏感特质，加密系统特别适合用于病人记录。但是，所述的加密系统及方法也可应用刑如银行户口，互联网客户户口，及其它传送及使用于互联网或只于一处理器。

术语表

非对称的密钥加密

一个加密系统利用第一把公用密钥把数据加密和第二把私人密钥把数据解码

属性/信息组

一个范畴的数据存储在一个目标

商务逻辑部件 (BLC)

一个电脑系统的组成部分而该组成部分能被客户端进入而制定和变更控制系统操作的商务规则和什么数据可以或不可以加密

核证管理员 (CM)

控制有关于核证机关操作和通信的系统密钥 PKI，而核证机关为系统密钥承担发行和核实数字认证

密文

加密的数据

类别

根据面向对象程序设计 而定的，对象的范畴

数据库适配器 (DBAD)

软件部件，该软件部件允许安全论域部件在不同型式的和由多个组成的数据库去存储和检索数据

数据加密标准 (DES)

对称的密钥保护方法利用 64-比特密钥

解密

由密文数据变更成明文

数字认证

电子通信的附件用于安全目的，一个典型的数字认证包含持有人资讯、一把公钥、认证发行人和认证的顺序码

加密

数据翻译成机密的密码

加密密钥管理员 (EKM)

一个电子计算机软件部件，而该软件部件管理对话加密密钥包含产生、取代和其他的任务

容错

一个系统在偶发事件中预料之外的硬体或软体故障时的持续操作能力。许多的容错电子计算机系统映照/复制整个的操作

一般的安全管理员 (GSM)

一个软件部件，而该软件部件是安全论域的操作监视者和进行散列、加密、解密的功能

硬体随机号码生成器 (HRNG)

一个装置用来为 SEKID 生成随机的号码

散列

由字符串生成一个号码，而该号码是基本上比文本它本身少。该散列值是不能逆转的加密，而该散列值的结果是不能逆转的。那个散列值或完整性值是用来检索查询和完整性安全核对用的。

网际协议 (IP)

具体说明资讯的格式和在互联网上传递资讯的寻址体制

网际协议安全 (IPSEC)

一套协议用来维持在网际协议层使资讯交换安全

IP 哄骗

试图制造一个通信看来好像来至经认可的网际协议地址

密钥

一个口令或表用来解码已加密的数据

密钥检查管理员 (KAM)

维持一个主动调节的日志关于一切的 EKM 和 SKM 的操作，而能够根据政策和定则发送警报和通报给收受者

密钥有效期管理员 (KLM)

监察 SEK 的权利失效和停止失效的 SEK 的使用或可选择在下一个要求或召唤时失效已标志的 SEK

记忆体 (RAM)

随机存取记忆内容

资讯整理 5 (MD5)

一个单方向的散列函数值，意味着该函数值接受一个资讯和转化成一个固定串列的数字，还可以叫资讯整理

对象

一个自身包含的统一体，而该统一体包含数据和步骤用来操纵数据

面向对象

有关于特别类型的编程，该编程把数据结构和功能结合起来创作可复用的对象

明文

非加密的数据

公钥基础建设

一个数字认证、核证机关和其他的注册机关的系统，该系统核实和认证网际交易的参与者的合法性和身分

安全的散列演算法

另一个单方向的散列函数值

安全密钥数据库 (KEYDB)

一个数据库在安全论域内部，SEK 和 SEKID 是储存在安全论域内部

安全承口层 (SSL)

一个为通过公用网际传递安全的资讯的协议发展

会话加密密钥 (SEK)

一个循环和动态的加密密钥用来加密数据统一体

会话加密密钥身分证明 (SEKID)

一个 SEK 的随机生成的身分证明号码

聪明卡

一个电子装置大约信用卡的大小含有电子记忆内容，它可以含有合成电路
对称的密钥加密

一个加密系统利用一把密钥把数据加密和解码的系统
系统密钥

一个 PKI 密钥用来加密和解码 SEKID

系统密钥共有的名字 (SKCN)

系统密钥数字认证顺序号码和主体共有的名字

系统密钥管理员 (SKM)

管理该系统密钥包含产生、核查和其他的任务
虚拟私有网络

一个网络利用公众的连接结点而建设

X. 509

一个广泛地利用的标准用来定义数字认证

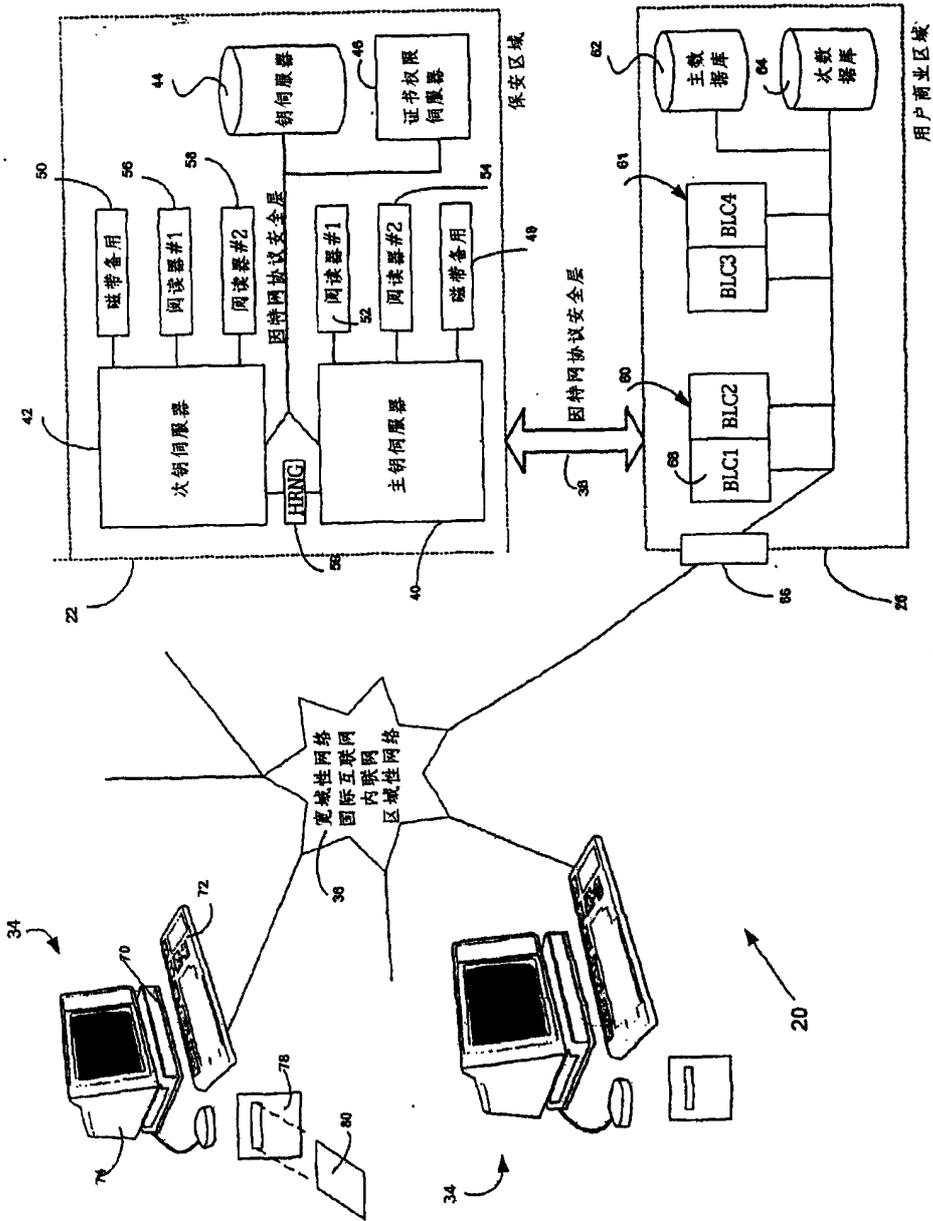


图1

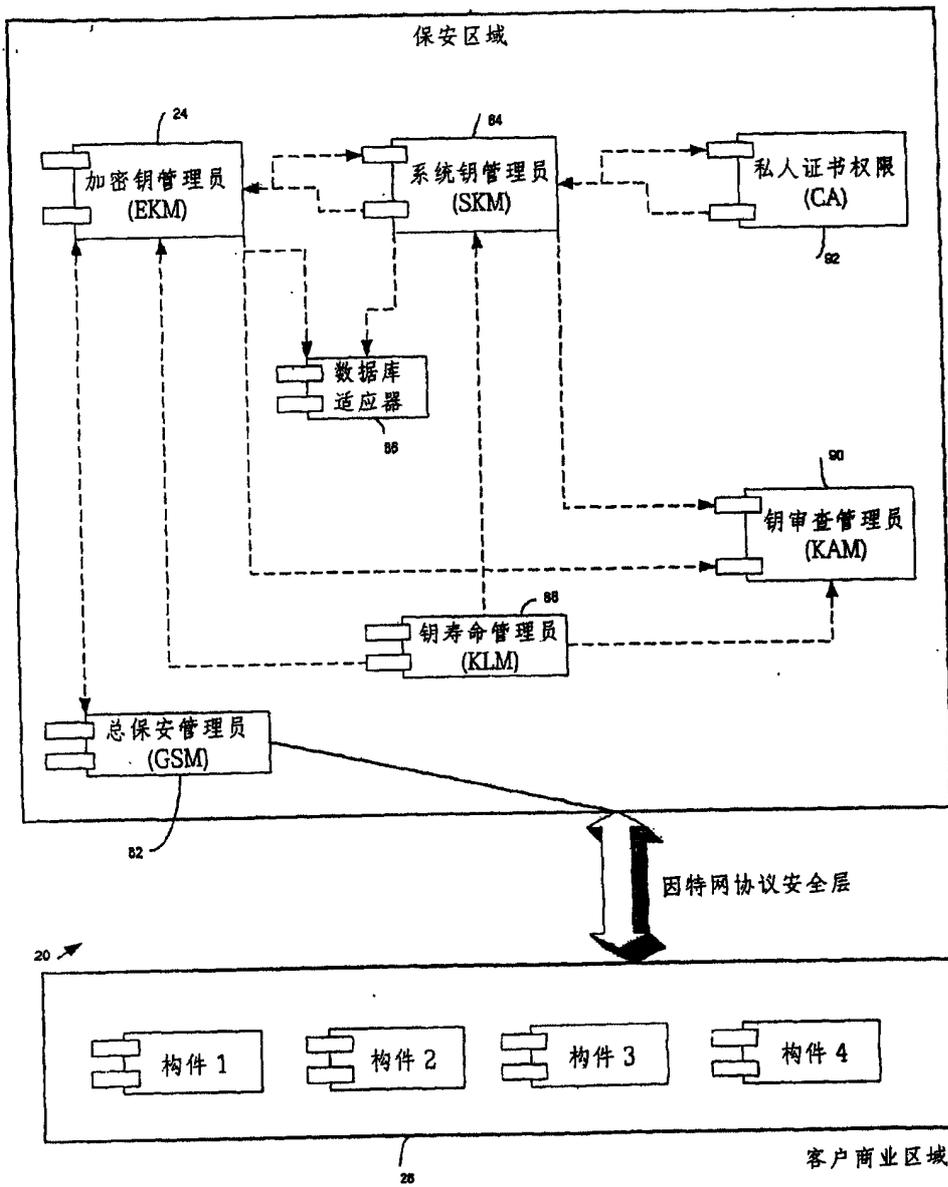


图2

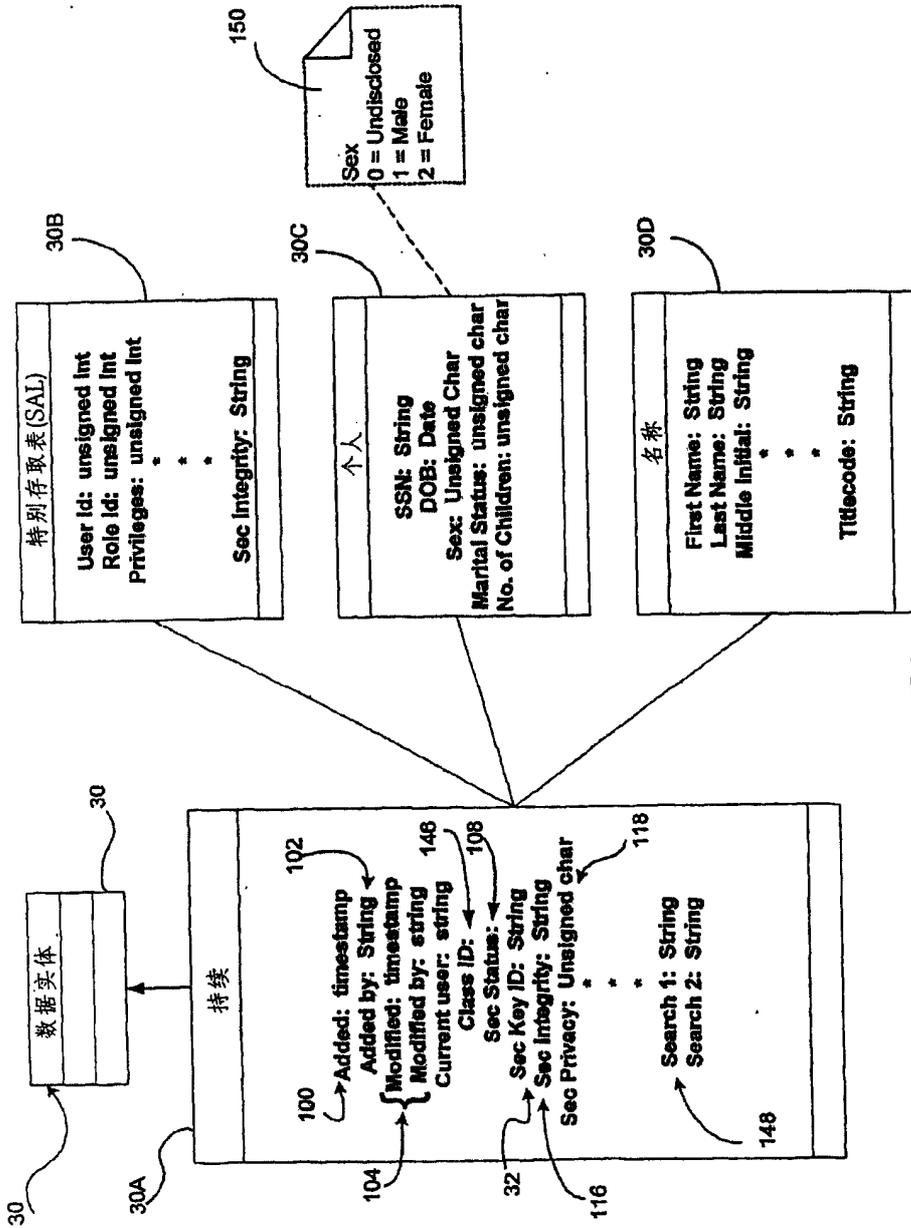


图 3

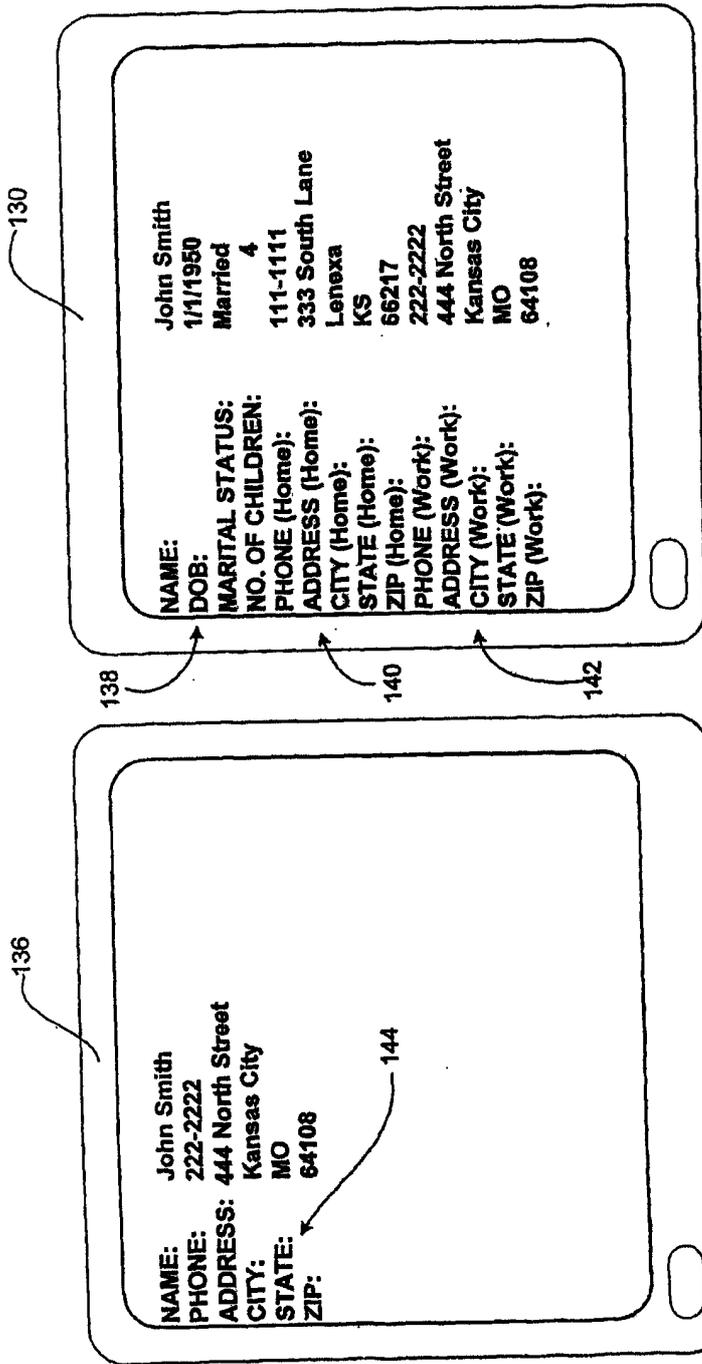


图5

图6

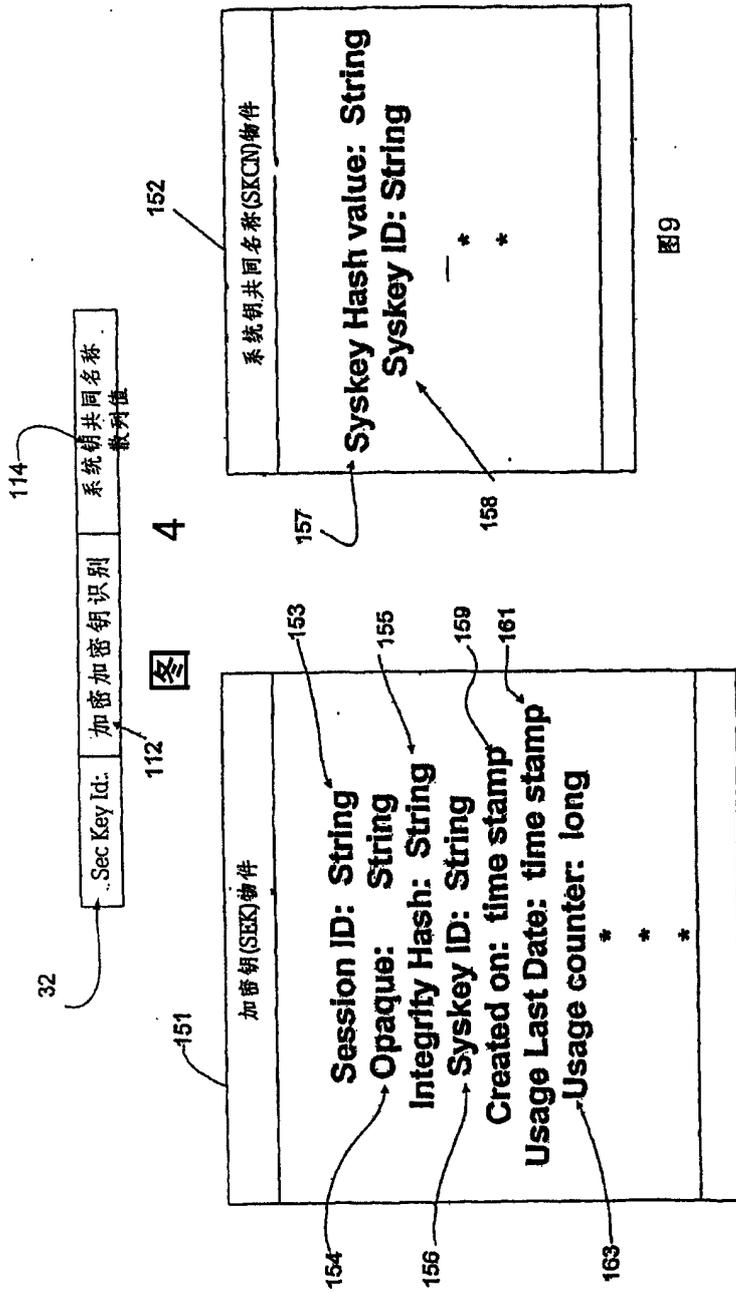


图8

图9

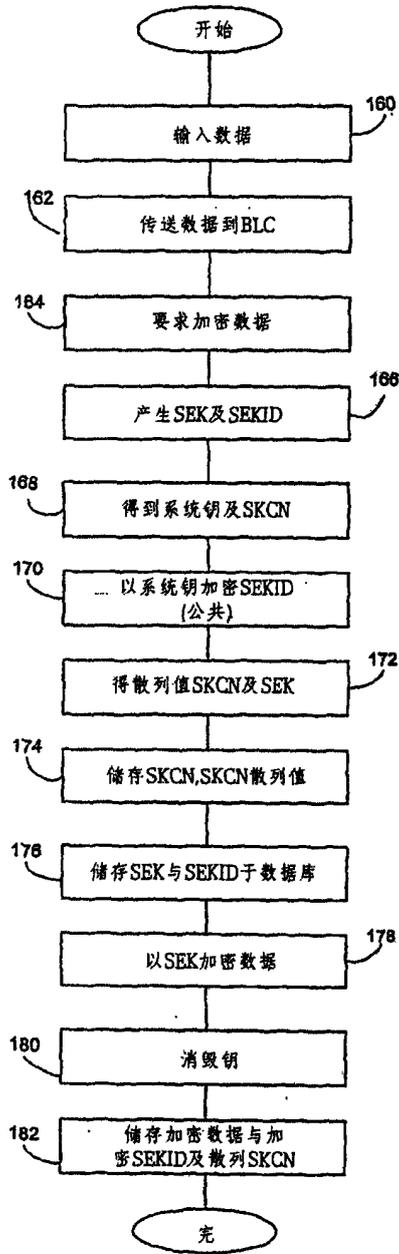


图 10

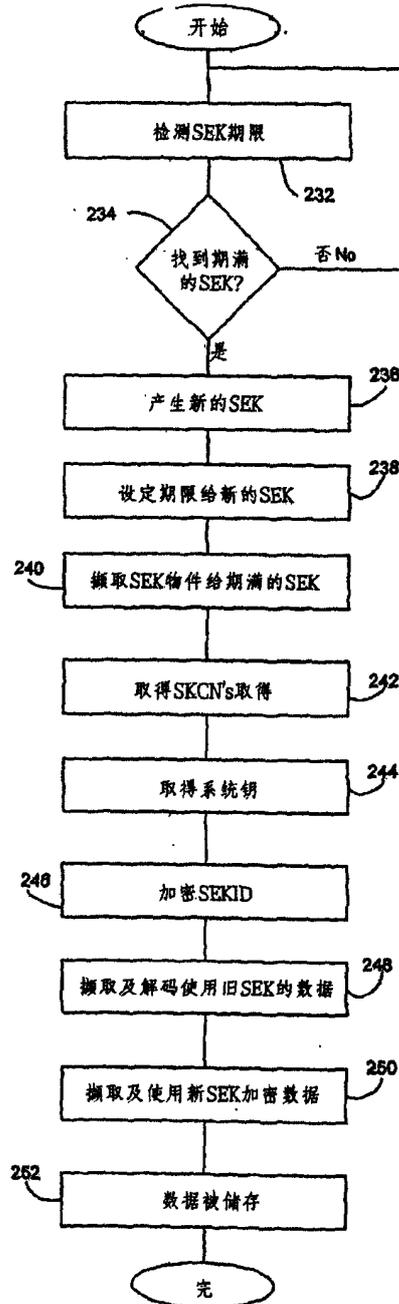


图 13

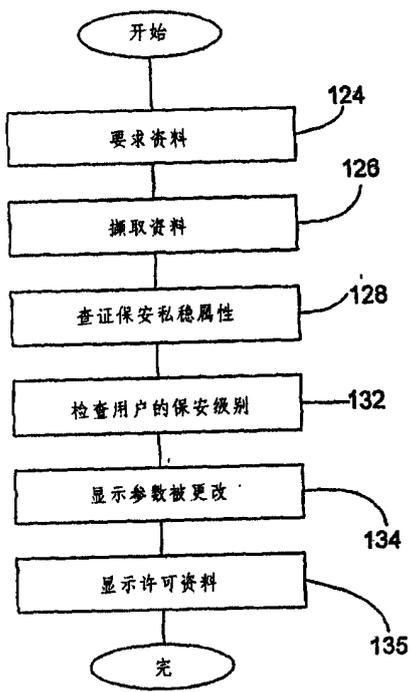


图 7

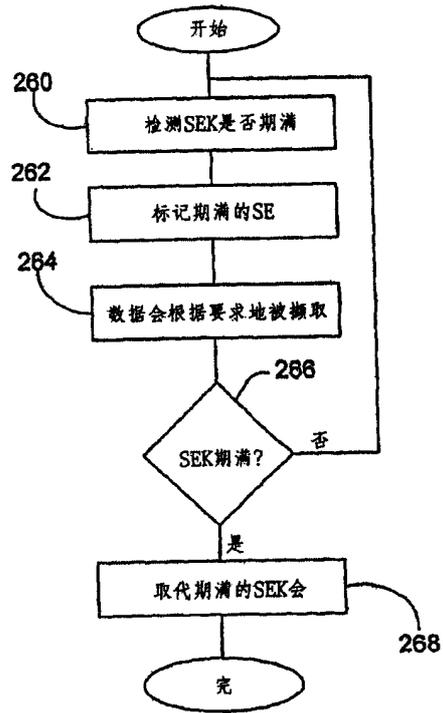


图 14

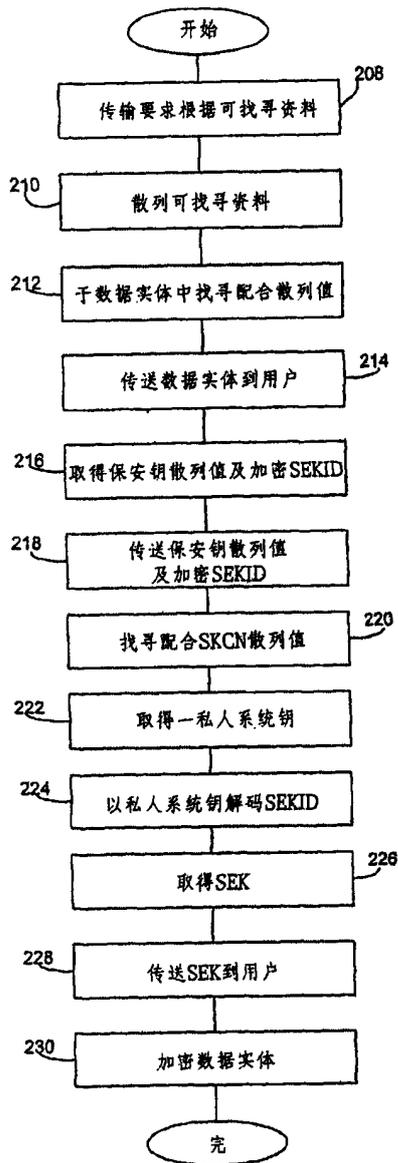


图 12

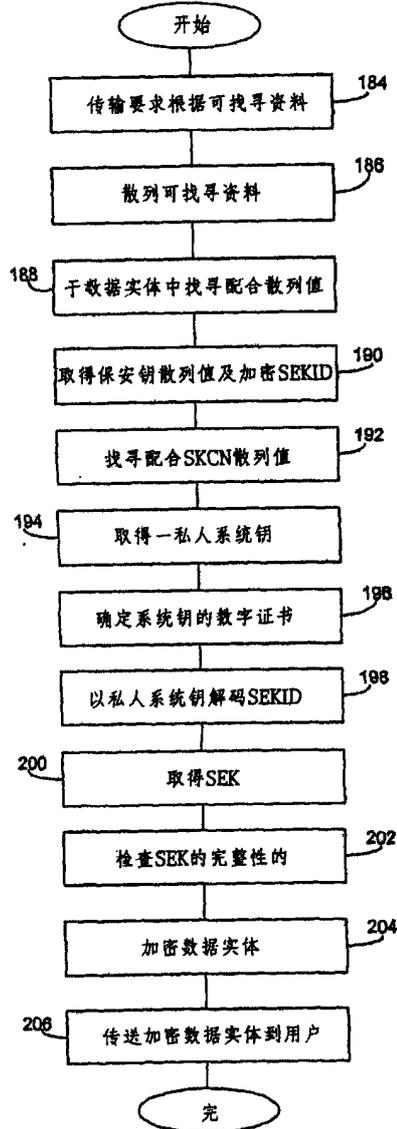


图 11