[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)
G06F 3/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610129101.4

[43] 公开日 2007 年 3 月 28 日

[11] 公开号 CN 1937492A

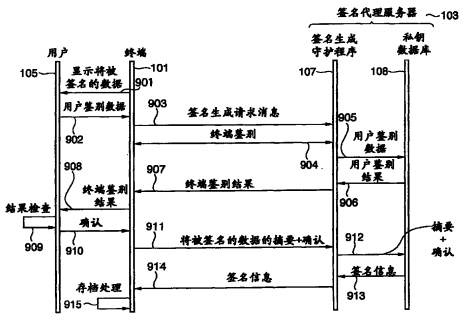
[22] 申请日 2006.9.8
[21] 申请号 200610129101.4
[30] 优先权
[32] 2005. 9. 9 [33] JP [31] 2005 - 262989
[71] 申请人 佳能株式会社
地址 日本东京
[72] 发明人 须贺祐治
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 董 莘
权利要求书 4 页 说明书 18 页 附图 11 页

[54] 发明名称

信息处理设备及其控制方法

[57] 摘要

为了提供一种即使在本地终端的可靠性未知时也能安全地生成签名的机制，本发明使得可能安全地通知用户远程服务器是否可以信任本地终端。 该机制包括用于接受来自用户终端的对于数字签名的生成请求的请求接受单元，鉴别用户终端的终端鉴别单元，鉴别已经经由用户终端发送该生成请求的用户的用户鉴别单元，以及基于来自终端鉴别单元和用户鉴别单元的鉴别结果，通知该用户终端对于该生成请求的应答的通知单元。



1. 一种信息处理设备，包括：

用于接受来自用户终端的对于数字签名的生成请求的请求接受单元；

用于鉴别所述用户终端的终端鉴别单元；

用于鉴别经由所述用户终端发送所述生成请求的用户的用户鉴别单元；以及

用于基于来自所述终端鉴别单元和所述用户鉴别单元的鉴别结果，向所述用户终端通知对于所述生成请求的应答的通知单元。

2. 根据权利要求 1 的设备，进一步包括：

用于响应所述生成请求，搜索数据库中存储的私钥的搜索单元；

从所述用户终端接收将被签名的数字文档的接收器；

用于通过利用所述私钥，生成将被签名的数字文档的数字签名的签名生成单元；以及

将所述数字签名发送到所述用户终端的发送器。

3. 根据权利要求 2 的设备，其中，

所述数据库存储与多个标识符相关的私钥，每个所述标识符识别所述私钥的用户，

所述搜索单元搜索与所述多个标识符中的第一标识符相关的私钥，其中所述第一标识符包含在生成请求中，以及

如果与所述第一标识符相关的私钥被存储在所述数据库中，则所述用户鉴别单元将所述用户鉴别为授权用户。

4. 根据权利要求 3 的设备，其中如果所述终端鉴别单元将用户终端鉴别为授权终端，并且所述用户鉴别单元将用户鉴别为授权用户，则所述通知单元通过将所述多个标识符中的第二标识符嵌入到应答中

来执行所述通知步骤。

5. 根据权利要求 3 的设备，其中如果所述终端鉴别单元没有将所述用户终端鉴别为授权终端，或者如果所述用户鉴别单元没有将所述用户鉴别为授权用户，则所述通知单元通过在应答中不嵌入任何一个所述多个标识符来执行所述通知步骤。

6. 根据权利要求 3-5 的任意一项的设备，其中

所述接收器还接收用于指定所述私钥的信息，以及

所述签名生成单元确定所述接收的信息是否与所述多个标识符中的第三标识符相匹配，并且如果确定所述接收的信息与所述第三标识符匹配，则生成数字签名。

7. 根据权利要求 2-4 的任意一项的设备，其中

所述接收器接收将被签名的数字文档连同对于数字签名的生成请求，以及

所述发送器在发送数字签名连同应答的通知时，加密并发送所述数字签名。

8. 根据权利要求 1 到 4 的任意一项的设备，其中所述通知单元发送应答到不同于已经发送生成请求的第一用户终端的第二用户终端。

9. 根据权利要求 8 的设备，其中所述第一标识符、第二标识符和第三标识符是相同的标识符。

10. 一种信息处理设备的控制方法，包括：

请求接受步骤，用于接受来自用户终端的对于数字签名的生成请求；

终端鉴别步骤，用于鉴别所述用户终端；

用户鉴别步骤，用于鉴别已经经由所述用户终端发送所述生成请求的用户；以及

通知步骤，用于基于来自所述终端鉴别步骤和所述用户鉴别步骤的鉴别结果，向所述用户终端通知对于所述生成请求的应答。

11. 根据权利要求 10 的方法，进一步包括：

搜索步骤，用于基于所述生成请求，搜索数据库中存储的私钥；

接收步骤，用于从所述用户终端接收将被签名的数字文档；

签名生成步骤，用于通过利用私钥，生成将被签名的数字文档的数字签名；以及

发送步骤，用于将所述数字签名发送到所述用户终端。

12. 根据权利要求 11 的方法，其中

所述数据库存储与多个标识符相关的私钥，所述多个标识符的每一个识别所述私钥的用户，

在搜索步骤中，搜索与所述多个标识符中的第一标识符相关的私钥，其中所述第一标识符被包含在所述生成请求中，以及

在所述用户鉴别步骤，如果与所述第一标识符相关的私钥被存储在所述数据库中，则所述用户被鉴别为授权用户。

13. 根据权利要求 12 的方法，其中如果在所述终端鉴别步骤中所述用户终端被鉴别为授权终端，并且在所述用户鉴别步骤中所述用户被鉴别为授权用户，则通过将所述多个标识符中的第二标识符嵌入到应答中，在所述通知步骤中执行通知。

14. 根据权利要求 12 的方法，其中如果在所述终端鉴别步骤中所述用户终端没有被鉴别为授权终端，或者在所述用户鉴别步骤中所述用户没有被鉴别为授权用户，则通过在应答中不嵌入任何一个所述

多个标识符，在所述通知步骤执行通知。

15. 根据权利要求 12-14 的任意一项的方法，其中

在所述接收步骤中还接收用于指定私钥的信息，以及

在所述签名生成步骤中，确定所述接收的信息是否与所述多个标识符中的第三标识符匹配，并且如果确定所述接收的信息与所述第三标识符匹配，则生成所述数字签名。

信息处理设备及其控制方法

技术领域

本发明涉及一种信息处理设备及其控制方法。

背景技术

近年来，随着计算机和其网络的迅速发展和普及，诸如文本数据、图像数据、音频数据等的多种类型的信息已经被数字化。数字数据不会由于老化或类似事情而损坏，并且可以永久地以理想状态保存。另外，数字数据可以很容易被复制、编辑和修改。

数字数据的这种复制、编辑和修改对用户非常有用，然而，数字数据的保护提出一个严峻的问题。特别是当文档和图像数据经由广域网，比如因特网和类似网络分发时，由于数字数据容易改变，第三方可能窜改该数据。

为了使接受方能校测输入数据是否已经被窜改，已经提出一种称为数字签名的处理技术作为用于检验附加数据以防止窜改的方案。这种数字签名处理技术不仅能够防止数据窜改，而且能够防止因特网上的电子欺骗、拒绝以及类似事情。

下面将详细描述数字签名、散列函数、公钥密码系统以及公钥基础设施（PKI）。

[数字签名]

图 10A 和图 10B 是用于说明签名生成处理和签名校验处理的视图，下面将参照图 10A 和图 10B 描述这些处理。在生成数字签名数据时，使用散列函数和公钥密码系统。

令 Ks（2106）为私钥，而 Kp（2111）为公钥。发送方对数据 M（2101）应用散列处理 2102 以计算摘要值 H（M）2103 作为定长数据。

接下来，发送方利用私钥 Ks（2106）对定长数据 H（M）应用签名处理 2104，以生成数字签名数据 S（2105）。发送方将该数字签名数据 S（2105）和数据 M（2101）发送到接受方。

接受方利用公钥 Kp（2111）转换（解密）所接收的数字签名数据 S（2110）。接受方通过对接收的数据 M（2107）应用散列处理 2108 生成定长摘要值：H（M）2109。校验处理 2112 校验解密的数据是否与该摘要值 H（M）匹配。如果作为该校验的结果，这两个数据不匹配，则可以检测到该数据已经被窜改。

在数字签名中，使用诸如 RSA、DSA（将在下文中祥述）等公钥密码系统。这些数字签名的安全性基于以下事实：除了私钥的持有者之外的实体很难根据计算来伪造签名或解码私钥。

[散列函数]

下面将描述散列函数。散列函数与数字签名处理一起使用，以便通过对将被签名的数据应用有损耗的压缩来缩短用于分配签名的处理时间周期。也就是说，散列函数具有处理具有任意长度的数据 M，以及生成具有恒定长度的输出数据 H（M）的功能。需要注意的是，输出 H（M）被称为明文数据 M 的散列数据。

特别地，单向散列函数的特征在于，如果给出数据 M，很难根据计算量来计算满足 H（M'）= H（M）的明文数据 M'。作为单向散列函数，诸如 MD2、MD5、SHA-1 等的标准算法是可用的。

[公钥密码系统]

下面将描述公钥密码系统。公钥密码系统利用两种不同的密钥，其特征在于，由一个密钥加密的数据只能由另一个密钥解密。在这两个密钥中，一个密钥被称为公钥，其对公众公开。另一个密钥被称为私钥，其由确定的人拥有。

利用公钥密码系统的数字签名、RSA 签名、DSA 签名、Schnorr 签名等类似签名是已知的。在此情况下，将举例说明在 R.L.Rivest，

A.Shamir 和 L.Aldeman: "A method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v.21, n.2, PP.120-126, Feb. 1978 中描述的 RSA 签名。同样，将另外说明在 2000 年 1 月的联邦信息处理标准(FIPS)186-2,数字签名标准(DDS)中描述的 DSA 签名。

[RSA 签名]

生成素数 p 和 q，以使 n = pq。λ(n)被设置为 p-1 和 q-1 的最小公倍数。选择对于λ(n)的适当的素数 e 以得到私钥 d = 1/e(mod λ(n))，在此 e 和 n 为公钥。而且，令 H( ) 为散列函数。

[RSA 签名生成] 用于文档 M 的签名生成序列

令 s:= H(M)^d(mod n)为签名数据。

[RSA 签名校验] 用于文档 M 的签名(s, T)的校验序列。

校验是否 H(M) = s^e (mod n)。

[DSA 签名]

令 p 和 q 为素数，而 p-1 为除尽 q 的值。令 q 为级数(order)q 的元(生成器)，它是从 Z_p*(将 0 从级数 p 的循环群 Z_p 中排除的乘法群)任意选择的。令任意从 Z_p*中选择的 x 为私钥以通过 y:= g^x mod p 给出公钥 y。令 H( ) 为散列函数。

[DSA 签名生成] 用于文档 M 的签名生成序列

1) α是从 Z_p 中任意选择的，以得到 T: = (g^α mod p) mod q。

2) 我们得到 C:= H(M)。

3) 我们得到 s:= α^-1(c+xT) mod q，以设置(S, T)为签名数据。

[DSA 签名校验] 用于文档 M 的签名(S, T)的校验序列

校验是否 T = (g^(h(M) s^-- 1) y^ (T s^- 1) mod p) mod q。

[公钥基础设施]

为了访问客户机-服务器通信中的服务器中的资源，需要用户鉴别。

作为用户鉴别的一种手段，普遍使用诸如 ITU-U 建议 X.509 等的公钥认证。公钥认证是保证公钥和其用户之间的绑定的数据，其由称为认证机构：CA 的信任的第三方数字签名。利用在浏览器中使用的 SSL（加密套接字协议层）的用户鉴别方案，是通过确认该用户是否具有对应于包含在由用户提供的公钥认证中的公钥的私钥来实现的。

由于公钥认证是由 CA 签名的，其中包含的用户或服务器的公钥是可以信任的。由于这个原因，当由 CA 在签名生成中使用的私钥泄漏或者变得容易受到攻击时，由该 CA 发出的所有公钥认证变得无效。由于一些 CA 管理大量的公钥认证，已经提出了各种建议用以降低管理成本。之后将描述的本发明能够减少要发出的认证以及作为公钥库的服务器访问的数量，作为其效果。

在 ITU-U 建议 X.509/ISO/IEC 9594-8 中描述的 ITU-U 建议 X.509 v.3 中："Information technology- Open Systems Interconnection-The Directory: Public-key and attribute certificate frameworks"，要被认证的实体（主题）的 ID 和公钥信息被包括作为要签名的数据。通过对将被签名的这些数据应用散列函数所获得的摘要进行签名操作，比如前述的 RSA 算法或类似算法，生成了签名数据。将被签名的数据具有可选字段"扩展"，该字段可包括对于应用或协议唯一的扩展数据。

图 11 示出了由 X.509 v.3 指定的格式，下面将说明每个字段中示出的信息。"版本"字段 1501 存储了 X.509 的版本。该字段是任选的，且如果省略，则代表 V1。"序列号"字段 1502 存储了由 CA 唯一分配的序列号。"签名"字段 1503 存储了公钥认证的签名方案。"发布者"字段 1504 存储了作为公钥认证的发布者的 CA 的 X.500 标识名称。"有效性"字段 1505 存储了公钥的有效周期（开始日期和结束日期）。

"主题"字段 1506 存储了对应于该认证中包含的公钥的私钥持有者的 X.500 标识名称。"主题公钥信息"字段 1507 存储了被认证的公钥。"发布者唯一标识符"字段 1508 和"主题唯一标识符"字段 1509 是从 V2 开始添加的任选字段，其分别存储 CA 和持有者的唯一标识符。

"扩展"字段 1510 是在 V3 中添加的任选字段，其存储了三值的集

合，即，扩展类型（extnId）1511、关键位（critical）1512 和扩展值（extnValue）1513。V3“扩展”字段不仅可以存储由 X.509 指定的标准扩展类型，还可以存储唯一的、新的扩展类型。由于这个原因，如何识别 V3“扩展”字段取决于应用方。关键位 1512 指示该扩展类型是不可缺少的还是可以忽略的。

已经描述了数字签名、散列函数、公钥密码系统和公钥基础设施。

由于上文描述的数字签名处理技术是基于公钥密码系统的，因此用于签名生成和签名校验的计算量极大。特别地，诸如 PDA 的便携式终端具有这样的问题，即，基于公钥密码系统的鉴别方法的计算成本高于普通 PC 的计算成本。因此，提出一种鉴别代理方法，其允许即使是低端的便携式终端也能利用由认证机构鉴别的认证执行信息通信，并减轻了例如由多个认证机构发布的认证的校验和管理的操作负担。（日本专利公开 N0.2001-197055）。

在这种提出的方法中，用户终端不需要任何认证校验功能或数字签名功能，并可以与高安全性的设备或系统交换数据。还提供了一种机制，其中该用户终端具有生物统计学数据输入单元，例如用于输入具有生物统计学能力的指纹，以及校验输入的生物统计学信息的鉴别代理服务器。这就使得即使当用户终端被盗或丢失时，也能够可靠地避免未授权的第三方使用数据。

如上所述，数字签名处理技术具有防止因特网上的电子欺骗、数据窜改、拒绝、以及类似问题的效果，并且还提供用于分发公钥认证的基础设施作为可靠性基础设施。最近，各种装置都利用这种可靠性基础设施，即，不仅 PC 和服务器，而且家用电子信息设备和蜂窝电话都利用这种可靠性基础设施。然而，利用可靠性基础设施的装置对用户时常不是必定可靠的。例如，用户通常使用的便携式终端和办公室 PC 包含用户的私钥，因而用户可以可靠地使用它们。另一方面，用户可能有时候使用一个可靠性无法被校验的装置。实例是可被第三方使用的公用电话亭终端、本地 PC 以及多功能的外围设备。用户必须小心，尤其在利用他或她的私钥执行处理时，即，在类似这样的情形中执行签名生成处理。

该签名生成处理需要用户的私钥，其通常存储在可靠的本地机器的硬盘或便携式 USB 道尔芯片（dongle）内。另一方面，当签名通过上述的公用电话亭终端、本地 PC 或多功能外围设备生成或扫描的文档时，用户需要能够安全地加载私钥的接口。即使当该装置具有私钥加载接口时，仍然存在这样的威胁，即用户在一个不同于将被签名的想要文档的文档上签名，即，即使将被签名数据的显示在屏幕上，用户也会面临签名被窜改的文档的威胁。

上文提出的方法提供了通过代理执行签名而不携带任何私钥的机制。然而，在这种方法中，即使在正确地鉴别用户时，远程终端通过代理执行签名而不了解该用户是否信任本地终端。

发明内容

因此，本发明使得能够安全地通知用户远程终端是否可以依赖本地终端，以便提供一个即使在可靠性未知的本地终端上也能安全地生成签名的机制。

根据优选实施例的一个方面的本发明涉及一种信息处理设备，包括适合于接受来自用户终端的对于数字签名的生成请求的请求接受单元，适合于鉴别用户终端的终端鉴别单元，适合于鉴别已经经由用户终端发送该生成请求的用户的用户鉴别单元，以及适合于基于来自终端鉴别单元和用户鉴别单元的鉴别结果，通知该用户终端对该生成请求的应答的通知单元。

根据优选实施例的另一方面的本发明涉及信息处理设备的控制方法，包括接受来自用户终端的对于数字签名的生成请求的请求接受步骤，鉴别用户终端的终端鉴别步骤，鉴别已经经由用户终端发送该生成请求的用户的用户鉴别步骤，以及基于来自终端鉴别步骤和用户鉴别步骤的鉴别结果，通知该用户终端对该生成请求的应答的通知步骤。

此外，通过以下示例性实施例（参照附图）的描述，本发明的其它特性将变得显而易见。

附图说明

图 1 是说明对应于本发明的实施例的系统的配置实例的示意图;

图 2 是说明当执行对应于本发明的实施例的签名处理时,显示屏的实例的示意图;

图 3 是说明对应于本发明的实施例的设备的硬件配置的实例的示意图;

图 4 是对应于本发明的实施例的数字文档生成处理的功能框图实例;

图 5 是对应于本发明的实施例的中间数字文档生成处理的流程图实例;

图 6A 是用于说明对应于本发明的实施例的中间数字文档和数字数据的示意图;

图 6B 是用于说明对应于本发明的实施例的中间数字文档和数字数据的示意图;

图 7 是对应于本发明的实施例的签名信息生成处理的流程图实例;

图 8 是说明对应于本发明的第一实施例的一系列签名代理处理的实例的示意图;

图 9 是说明对应于本发明的第三实施例的一系列签名代理处理的实例的示意图;

图 10A 是说明签名生成处理的一般实例的示意图;

图 10B 是说明签名校验处理的一般实例的示意图; 以及

图 11 是用于说明公钥认证 X.509 v.3 的数据格式的示意图。

具体实施方式

下面参考附图说明本发明的优选实施例。

[第一实施例]

该实施例将说明通过在借助于扫描纸件文档生成的图像数据上或在预存数字内容上生成数字签名,生成混合内容(在下文中称为数字文档)的数字文档生成处理。

图 1 是说明对应于该实施例的系统的实例的示意图。在图 1 所示的该系统中，生成数字文档的终端 101 和签名代理服务器 103 与网络 104 相连。用户 105 通过在终端 101 上执行签名处理，在终端 101 中存储的数字文档上、从与终端 101 相连的扫描器 102 输入的图像数据上、或数字文档和图像数据的混合内容上生成数字签名。

私钥是执行签名处理所必需的。作为这种私钥，可能使用存储在终端 101 中的私钥或使用从终端 101 的私钥加载接口加载的私钥。还可能通过网络从签名代理服务器 103 下载私钥。服务器 103 具有签名生成守护程序（程序）107 用于执行签名处理，并与私钥数据库 108 连接用于管理私钥。

图 2 是说明当用户 105 在终端 101 上执行签名处理时，终端 101 显示的显示屏的实例的示意图。参照图 2，显示屏 201 显示用于将被签名的数据的显示区域 202、私钥选择区域 203 以及用于执行签名处理的按钮 204。用户 105 可以通过在用于将被签名的数据的显示区域 202 中确认将被签名的数据，在私钥选择区域 203 中选择私钥，并按下用于执行签名处理的按钮 204 来执行签名处理。

私钥选择区域 203 可以选择以下三种方法：（1）使用存储在终端 101 中的私钥的方法；（2）从终端 101 的私钥加载接口获取私钥的方法；以及（3）通过网络 104 从签名代理服务器 103 下载私钥的方法。需要注意的是，即使对于相同的方法，多个私钥有时被存储在终端 101 中，或有时存在多个私钥输入接口。此外，可以存在多个不同的签名代理服务器。因此，为每种方法显示多种选择。

特别地，方法（3）使用签名代理服务器 103 中的签名生成守护（程序）107 和私钥数据库 108。另外，用户 105 还可以使用通信装置，比如便携式终端 106，其使用与网络 104 不同的信道。

通过假定便携式终端 106 为利用另一个信道的通信装置进行以下说明。然而，可以使用任何装置，只要它是利用不同于网络 104 的信道的通信装置，并且可以将信息从签名代理服务器 103 传送到用户 105。实例有传真设备、固定电话、蜂窝电话、利用另一载体的电子邮件以及

邮件，但是本发明不局限于这些实例。

图 3 示出了终端 101 和签名代理服务器 103 的内部硬件配置的实例。CPU 301 通过执行软件控制大多数设备。存储器 302 临时存储要被 CPU 301 执行的软件以及数据。硬盘 303 存储软件和数据。输入/输出（I/O）单元 304 接收来自键盘、鼠标、扫描仪以及类似设备的输入信息，并输出信息到显示器或打印机。

[数字文档生成处理]

下面将说明对应于该实施例的数字文档生成处理。图 4 是示意了该实施例的数字文档生成处理的实例的功能框图。

在对应于该实施例的数字文档生成处理中，数字文档输入处理 402 输入数字文档 401。同样，纸件文档输入处理 404 输入纸件文档 403。中间数字文档生成处理 405 分析输入的纸件文档 403 并生成中间数字文档。中间数字文档、数字文档 401 以及私钥 406 被输入到签名信息生成处理 407 以生成签名信息。另外，签名信息附加处理 408 将中间数字文档、数字文档 401 以及签名信息相互关联。此外，数字文档生成处理 409 通过组合中间数字文档、数字文档 401 以及签名信息来生成数字文档 411。数字文档传送处理 410 将数字文档 411 发送到外界。

注意，所生成的和发送的数字文档 411 还可以作为数字文档 401 再次输入到数字文档输入处理 402 中，以再生新的数字文档 411。下面将说明各个功能框的细节。

首先，将说明图 4 所示的中间数字文档生成处理 405 的细节。图 5 是示意在对应于该实施例的中间数字文档生成处理 405 中的处理实例的流程图。

在步骤 S501，数字数据是通过将从纸件文档输入处理 404 获得的数据进行数字化而生成。在步骤 S502，数字数据与属性一一对应地被划分为多个区域。在此提及的属性的实例有字符、照片、表格以及线条画。

例如，区域划分处理可以从文档图像中提取一个诸如黑像素的 8 个连接的轮廓块（contour mass）或白像素的 4 个连接的轮廓块的集合，

并提取根据该集合的形状、大小、状态以及类似特性一个区域，比如表征该文档的字符、图片、图形、或表格。该方法例如在 U.S.P. NO. 5，680，478 中描述。需要注意的是，实现区域划分处理的方法并不局限于该方法，也可以使用另一种方法。

在步骤 S503，为在步骤 S502 获得的每个区域生成文档信息。文档信息的实例有属性、诸如页面的位置坐标的布局信息、如果划分的区域的属性是字符的字符代码串以及诸如段落和标题的文档逻辑结构。

在步骤 S504，在步骤 S502 获得的每个区域被转换成转印信息。转印信息是绘制所必需的信息。实际的实例有可变分辨率光栅图像、向量图像、单色图像、彩色图像、每个转印信息的文件大小，以及如果被划分的区域的属性是字符，则是作为字符识别的结果的文本。其它实例有每个字符的位置、字体以及通过字符识别获得的字符的可靠性。

在步骤 S505，在步骤 S502 划分的区域、在步骤 S503 生成的文档信息和在步骤 S504 获得的转印信息是彼此相关的。相关信息由树结构描述。在上述步骤生成的转印信息和文档信息在下文中将被称为组元（constituent element）。

在步骤 S506，在前一阶段生成的组元被保存作为中间数字文档。只要保存格式可以表示树结构，就不需要对于该树结构作出特定的限制。在这个实施例中，中间数字文档被以 XML 格式保存作为构建的文档的实例。

下面将描述签名信息生成处理 407。该处理为先前生成的中间数字文档的组元生成数字签名。图 7 是对应于该实施例的签名信息生成处理中的处理的流程图。下面参照图 7 说明签名信息生成处理 407。

在步骤 S801，生成将被签名的每个数据的摘要值。将被签名的数据是作为在中间数字文档中包含的签名对象的数据，并且当其被看作是图 6A 和 6B 所示的转印信息 a 701，转印信息 b 702，或文档信息 703（将在下文描述）时能够很容易地被理解。同样，这个实施例使用散列函数以生成摘要值。该散列函数已经在“背景技术”中说明，因此将省略其详细说明。

在步骤 S802，生成将被签名的每个数据的标识符。该标识符仅需要能够唯一地识别将被签名的数据。例如，该实施例使用由 RFC 2396 定义的 URI 作为将被签名的数据的标识符。然而，本发明不局限于这种标识符，并且多种值可以被用作标识符。

在步骤 S803 中，确定步骤 S801 和 S802 是否已经被应用于所有将被签名的数据。如果步骤 S801 和 S802 已经被应用于所有将被签名的数据（在步骤 S803 中为“YES”），则流程前进到步骤 S804；如果不是，该流程返回到步骤 S801。

在步骤 S804，通过利用私钥 406 对在步骤 S801 中生成的所有摘要值以及在步骤 S802 中生成的所有标识符执行签名处理，从而计算签名值。为计算该签名值，该实施例使用“背景技术“中说明的数字签名。例如，图 10A 和 10B 中所示的签名生成处理流程中的输入数据：M 2101 对应于在步骤 S801 中生成的所有摘要值以及在步骤 S802 中生成的所有标识符（该数据组在下文中将被称为聚合数据）。同样，私钥 Ks 2106 对应于私钥 406。需要注意的是，将省略对数字签名的实际操作的详细说明。

由在图 2 所示的私钥选择区 203 中选择的方法使用私钥 406。当从本地终端（终端 101）获取私钥 406 时，如同先前描述的那样处理私钥 406。随后将参照图 8 描述授权远程终端（签名代理服务器 103）执行签名处理的操作。

随后，在步骤 S805，通过利用该聚合数据（在步骤 S801 生成的所有摘要值和在步骤 S802 生成的所有标识符）以及在步骤 S804 生成的签名值，生成签名信息，从而完成签名生成处理。

下面将参照图 6A 说明签名信息附件处理 408 中的处理。附图标记 701 和 702 表示在中间数字文档生成处理 405 中生成的中间数字文档的转印信息；703 表示文档信息；而 704 和 705 表示在签名信息生成处理 407 中生成的签名信息。

如上所述，指示转印信息或文档信息为将被签名的数据的识别信息被嵌入在签名信息中。参照图 6A，指示将被签名的数据（即转印信息

701）的识别信息 706 被嵌入在签名信息 704 中。签名数据和将被签名的数据不需要一一对应。例如，分别指示将被签名的数据的转印信息 702 和文档信息 703 的识别信息 707 和 708 也可以嵌入在签名信息 705 中。

下面将参照图 6A 和 6B 说明数字文档生成处理 409。如图 6A 所示，存在在以上步骤中生成的中间数字文档和签名数据作为单个独立的数据。因此，数字文档生成处理通过将这些数据存档为一个数据来生成数字文档。图 6B 是说明中间数字文档和签名数据的存档数据的实例的示意图。存档数据 709 对应于图 4 所示的数字文档 411。同样，图 6A 所示的附图标记 701、702、703、704 和 705 分别对应于附图标记 713、714、712、710 和 711。

最后，数字文档发送处理 410 将数字文档 411 发送到外部。生成的数字文档 411 也可以作为数字文档 401 再次输入到数字文档输入处理，以再生新的数字文档 411。

上文已经说明了该实施例的数字文档生成处理。

[签名处理授权]

下面参照图 8 说明授权远程终端（签名代理服务器 103）执行签名处理的操作。图 8 是签名代理处理的一系列示意图，签名代理处理由用户 105、终端 101、签名生成守护程序 107 以及私钥数据库 108 之间的协议构成。

在 901，用户能够通过在显示区域 202 中显示将被签名的数据，确认将被签名的数据的内容。在对应于图 2 所示的显示实例的显示屏上，私钥选择区 203 显示“（3）使用签名代理服务器”，并且基于 URI 选择期望的签名代理服务器。当用户操作按钮 204 以执行签名处理时，执行自 902 的处理。

在 902，终端 101 从用户 105 接受输入的用户鉴别数据，作为允许签名代理服务器 103 鉴别和识别用户 105 的标识符。用户鉴别数据不仅可以通过从键盘输入口令字来输入，还可以根据终端的输入装置选择适当的数据来输入。当使用口令字时，可能不仅使用固定字，还可以使用

根据便携式终端的使用时间而改变的一次性口令字，或用以将签名生成权转移到不同的实体的一次性口令字。

在 903，终端 101 生成包含由用户 105 输入的用户鉴别数据的签名生成请求消息，并将该消息发送到签名代理服务器 103（实际上，签名生成守护程序 107 接受该消息）。签名生成请求消息还可以包含由签名代理服务器 103 管理的用户标识符。该用户标识符还可能受到对于登录到终端 101 的鉴别行为的限制。

在 904，签名代理服务器 103 执行终端鉴别，以确定作为签名生成请求消息的发送源的终端 101 是否可以被信任。该终端鉴别可以通过基于用户 105 的策略以及签名代理服务器 103 的方法执行。实例有利用公钥密码系统的鉴别方法、利用公钥认证和公钥基础设施的鉴别方法以及利用密钥密码系统的鉴别方法。

在 905，签名生成守护程序 107 分析所接收的签名生成请求消息，以提取用户鉴别数据，并将提取的数据发送到私钥数据库 108。904 和 905 可以并行或顺序地执行。

在 906，基于用户鉴别数据，确定是否存在期望的私钥，并且确定用户是否为授权用户。如果存在私钥且该用户是授权用户，则返回终端鉴别结果到签名生成守护程序 107。该终端鉴别结果包含对应于用户鉴别数据的数据。该终端鉴别结果是作为对应于在 902 由用户 105 输入的用户鉴别数据的标识符的信息，并且只要该用户可以确认该数据，该终端鉴别结果就可以采用任何形式。例如，可以使用预定口令字。

在 907，如果在 904 中通过终端鉴别确定终端 101 是可信任的终端，并且从私钥数据库 108 获得该终端鉴别结果，则签名生成守护程序 107 将终端鉴别结果发送到终端 101。另一方面，如果 904 中的终端鉴别失败，或没有从私钥数据库 108 获得终端鉴别结果，则签名生成守护程序 107 发送伪数据，而不是终端鉴别结果到终端 101。

在 908，终端 101 显示从签名代理服务器 103 接收的终端鉴别结果。如果终端 101 是未授权的终端，或者如果该用户是未授权的用户，则屏幕不会显示任何正确的信息。

在 909，用户 105 确定终端 101 上显示的终端鉴别结果的内容是否对应于在 902 输入的用户鉴别数据。虽然终端鉴别结果是以例如口令字的形式显示的，其还可以通过取决于终端 101 的显示功能的适当装置提供。在这种情况下，用户 105 还可以确认随机号码表中的对应关系。

在 910，如果他或她确定终端 101 是可信任的，则用户 105 输入一个确认到终端 101。这个确认不局限于从键盘输入的口令字，并且可以根据该终端的另一输入装置适当地选择。需要注意的是，当该确认为口令字时，就可能不仅使用固定口令字，还可以使用根据便携式终端使用的时间而改变的一次性口令字，或者是用于将签名生成权转移到不同实体的一次性口令字。该确认是与上述的用户鉴别数据和终端鉴别结果相关的标识符，并且用于确定用户 105 是否允许签名代理服务器 103 签名将被签名的数据。

在 911，终端 101 发送摘要和确认到签名生成守护程序 107，该摘要是通过利用散列函数在将被签名的数据上执行的操作的结果。还可能发送将被签名的数据而不是摘要。

在 912，签名生成守护程序 107 发送将被签名的数据或其摘要以及确认到私钥数据库 108。私钥数据库 108 搜寻与该确认相关的私钥。也就是说，私钥数据库 108 预先确定该确认是否与和私钥相关的用户 105 的标识符相匹配。如果该确认与用户 105 的标识符匹配，且存在私钥，则将被签名的数据或其摘要通过利用私钥签名，从而生成签名信息。

在 913，生成的签名信息被返回到签名生成守护程序 107，并在 914 发送到终端 101。在 915，终端 101 根据数字文档生成处理 409 将签名信息存档，从而生成数字文档 411。

下面将说明如果终端 101 是未授权的终端所执行的操作。如果终端 101 是未授权的终端，则签名代理服务器 103 在终端鉴别 904 检测该信息。于是，在 907 没有返回正确的终端鉴别结果。因此，在 909，用户 105 能够基于终端 101 上显示的内容，识别终端 101 是未授权的终端。这就允许用户中断随后的处理，即，利用私钥的远程签名处理。

即使终端 101 省略了从 908 到 910 的步骤，并在 911 发送未授权的

确认以请求用户 105 执行远程签名，只有用户 105 独自知道正确的确认。因此，即使搜寻到与该未授权的确认相关的私钥，也没有这种私钥，因此可能立即确定该确认是未授权的。这就允许签名代理服务器 103 检测未授权的终端，并停止生成签名信息。通过这种方式，就可能提供一种阻止通过未授权的终端形成签名信息，并安全地执行远程签名的机制。

上面说明了授权签名处理的操作。这个系统能够提供一种即使通过利用可靠性未知的本地终端也能安全地生成签名的机制。也就是说，可以安全地通知用户，指示远程服务器（签名代理服务器 103）是否可以信任本地终端（终端 101）的结果。因此，用户可以确定是否在确认本地终端的可靠性后使用本地终端。另外，这种机制可以通过仅仅利用描述口令字集合的随机号码表来实现，而不需要利用任何专用装置。这就有利地降低了安装的成本。

[第二实施例]

在上文说明的第一实施例中，签名处理的授权大致包括本地终端和远程终端之间的由附图标记 903、907、911 和 914 表示的四向协议。然而，因为签名信息被预先嵌入在终端鉴别结果中，这个实施例只需要双向协议。

这个实施例并不执行图 8 中 911 后的流程。取而代之的是，在 911 发送的将被签名的数据或其摘要，以及在 914 接收的签名信息同时在 903 和 907 被发送。

在 903，终端 101 发送签名生成请求消息和将被签名的数据或其摘要到签名代理服务器 103。将被签名的数据或其摘要还可以在 903 的发送之前发送。这就允许签名代理服务器 103 搜寻期望的私钥，并通过利用该私钥在 907 发送终端鉴别结果之前签名将被签名的数据或其摘要。在 906，私钥数据库 108 返回用户鉴别结果和签名信息到签名生成守护程序 107。

在 907，除了终端鉴别结果外，还可以发送签名信息。然而，因为终端 101 可能未授权，签名信息在加密后被发送。当在 910 用户 105 输

入确认到终端 101 时，终端 101 可以解密加密后的签名信息。

上述是利用由附图标记 903 和 907 表示的双向协议的实施例。这就使得可能通过简化的数据流程获得与第一实施例相同的效果。

[第三实施例]

上述的第一和第二实施例假设在图 8 的 908 中，被未授权的第三方窜改在终端 101 上显示的终端鉴别结果，因此用户必须管理三个相关的口令字。这三个口令字是用户鉴别数据、终端鉴别结果和确认。这也使得用于实现以上实施例的协议变复杂了。

因此，该实施例假定可由用户 105 信任的便携式终端 106 作为一个新的实体，并以便携式终端 106 上显示的数据可信任为前提，通过简化的协议构建一个系统。

图 9 是说明对应于该实施例的一系列签名代理处理的实例的示意图。参照图 9，便携式终端 106 被添加到图 8 所示的用户 105、终端 101、签名生成守护程序 107 和私钥数据库 108 中。下面将说明这个实施例的顺序。需要注意的是，这个实施例将说明第二实施例（双向协议）的修改，但是该实施例还可以类似地应用于第一实施例。

图 9 中的 1001 至 1006 与第二实施例中的 901 至 906 相同，所以将省略对其的说明，并且下面说明自 1007 的处理。

图 8 的 907 中的处理在图 9 中被划分成 1007a 和 1007b。在 1007a，加密的签名信息被发送到终端 101。在 1007b，终端鉴别结果被发送到可靠的便携式终端 106，而不是终端 101。如同在上述实施例中，终端鉴别结果还可以是先前与在 1002 输入的用户鉴别数据相关的另外数据。如果可能确认签名代理服务器 103 是发送源，则终端鉴别结果也可以与用户鉴别数据相同。

在 1008，如果用户 105 基于在 1007b 接收的终端鉴别结果确定终端 101 是可信任的，则用户 105 输入一个确认到终端 101。这个确认也可以经由 1007b 和终端鉴别结果一起传送到用户 105。在此情况下，用户 105 只需为一项事务处理管理一个口令字。

当从用户 105 接收到输入确认时，在 1009，终端 101 解密加密的签名信息。在 1010，终端 101 通过根据数字文档生成处理 409 存档数据来生成数字文档 411。

通过这种方式，可以减少由用户管理的口令字的数量。具体说，在第一和第二实施例中，用户必须为一项事务处理管理三个口令字。然而，在这个实施例中，用户只需为一项事务处理管理一个口令字。这大为改善了用户友好性。

<利用另一加密算法的实施例>

上述实施例没有提及任何加密（隐蔽）方法。然而，本发明不仅能容易地应用于利用公钥密码系统的加密方法，而且还能应用于利用密钥密码系统的加密方法。因此，本发明还包括上述实施例通过利用另一加密算法实现的情况。

<其它实施例>

注意本发明可应用于包含单个装置的设备或可以应用于由多个装置构成的系统。

此外，本发明可以通过为系统或设备直接或间接提供实现前述实施例的功能的软件程序，用该系统或设备的计算机读取提供的程序代码，然后执行该程序代码来实现。在此情况下，只要该系统或设备具有该程序的功能，实现模式不需要依赖程序。

因此，由于本发明的功能是通过计算机实现的，计算机中安装的程序代码也实现了本发明。换言之，为了实现本发明的功能的目的，本发明的权利要求还涵盖了计算机程序。

在此情况下，只要该系统或设备具有该程序的功能，该程序就可以以任何形式执行，比如目标代码、通过解释程序执行的程序、或提供给操作系统的脚本数据。

可以用于提供程序的存储介质的实例有软盘、硬盘、光盘、磁光盘，CD-ROM、CD-R、CD-RW、磁带、非易失型存储卡、ROM 以及 DVD

（DVD-ROM，DVD-R 或 DVD-RW）。

至于提供该程序的方法，可以利用客户计算机的浏览器将客户计算机连接到因特网上的网站，并且本发明的计算机程序或该程序的自动可安装压缩文件可以下载到诸如硬盘的记录媒介上。此外，本发明的程序可以通过将构成该程序的程序代码划分成多个文件并从不同的网站下载这些文件来提供。换言之，通过计算机将实现本发明的功能的程序文件下载到多个用户的 WWW（万维网）服务器也被本发明的权利要求书涵盖。

还可能加密本发明的程序并将该程序存储在诸如 CD-ROM 的存储介质上，将存储介质分配给用户，允许满足某些要求的用户经由因特网从网站下载解密密钥信息，并允许这些用户通过利用该密钥信息解密加密的程序，由此将该程序安装在用户计算机中。

除了根据这些实施例的上述功能通过由计算机执行所读取的程序来实现的情况之外，在计算机上运行的操作系统或类似物可以执行实际处理的全部或一部分，使得上述实施例的功能可以通过该处理实现。

此外，在从存储介质读出的程序写入到被插入在计算机中的功能扩展板或与计算机连接的功能扩展单元上提供的存储器之后，CPU 或安装在功能扩展板或功能扩展单元上的类似物执行实际处理的全部或一部分，使得前述实施例的功能可以通过该处理实现。

由于可以不偏离本发明的精神和范围实现本发明的许多明显大为不同的实施例，将理解的是，除了在所附权利要求中定义的之外，本发明不局限于其中的特定实施例。

图1

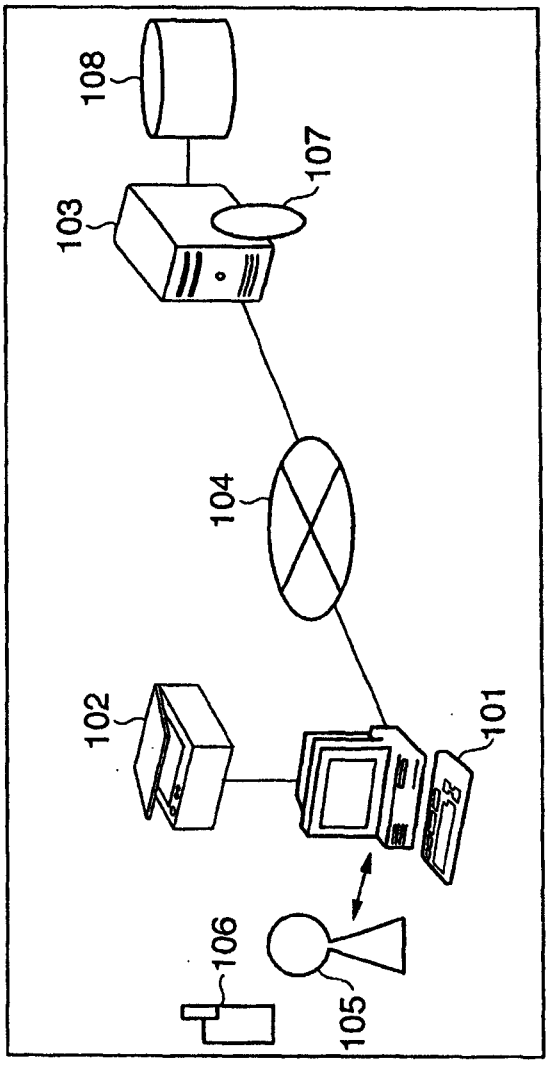


图2

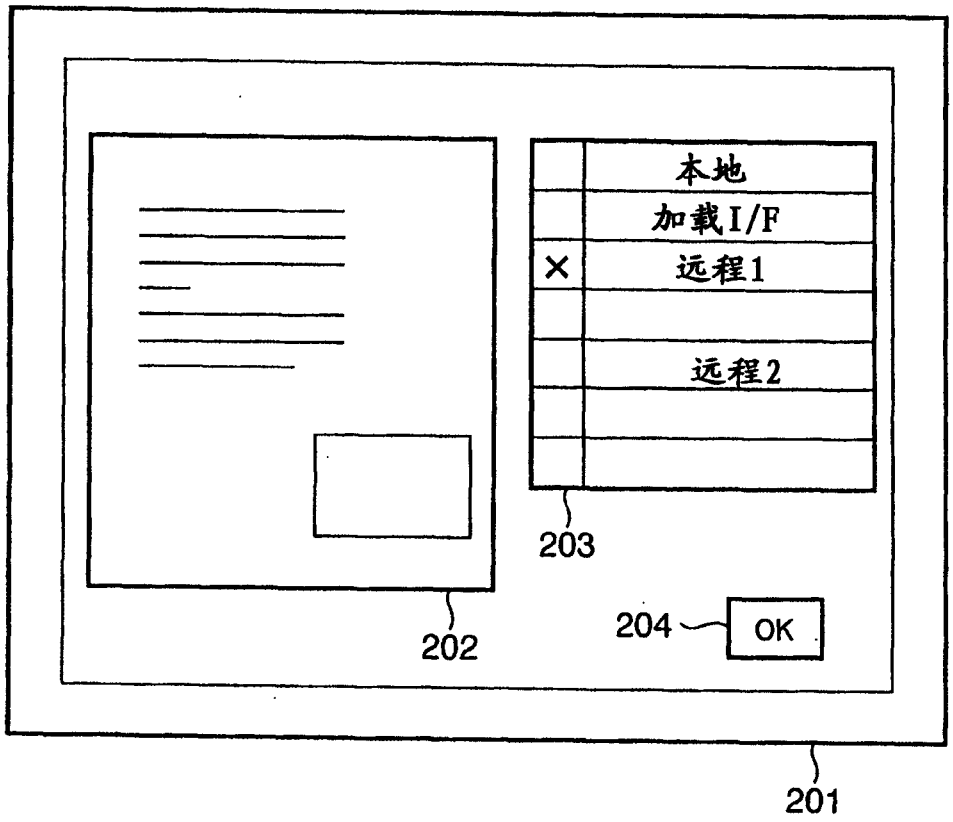


图 3

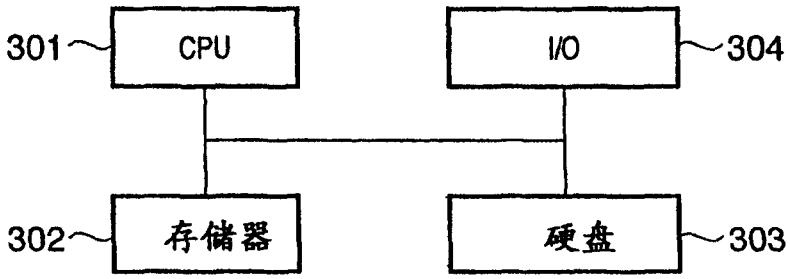


图4

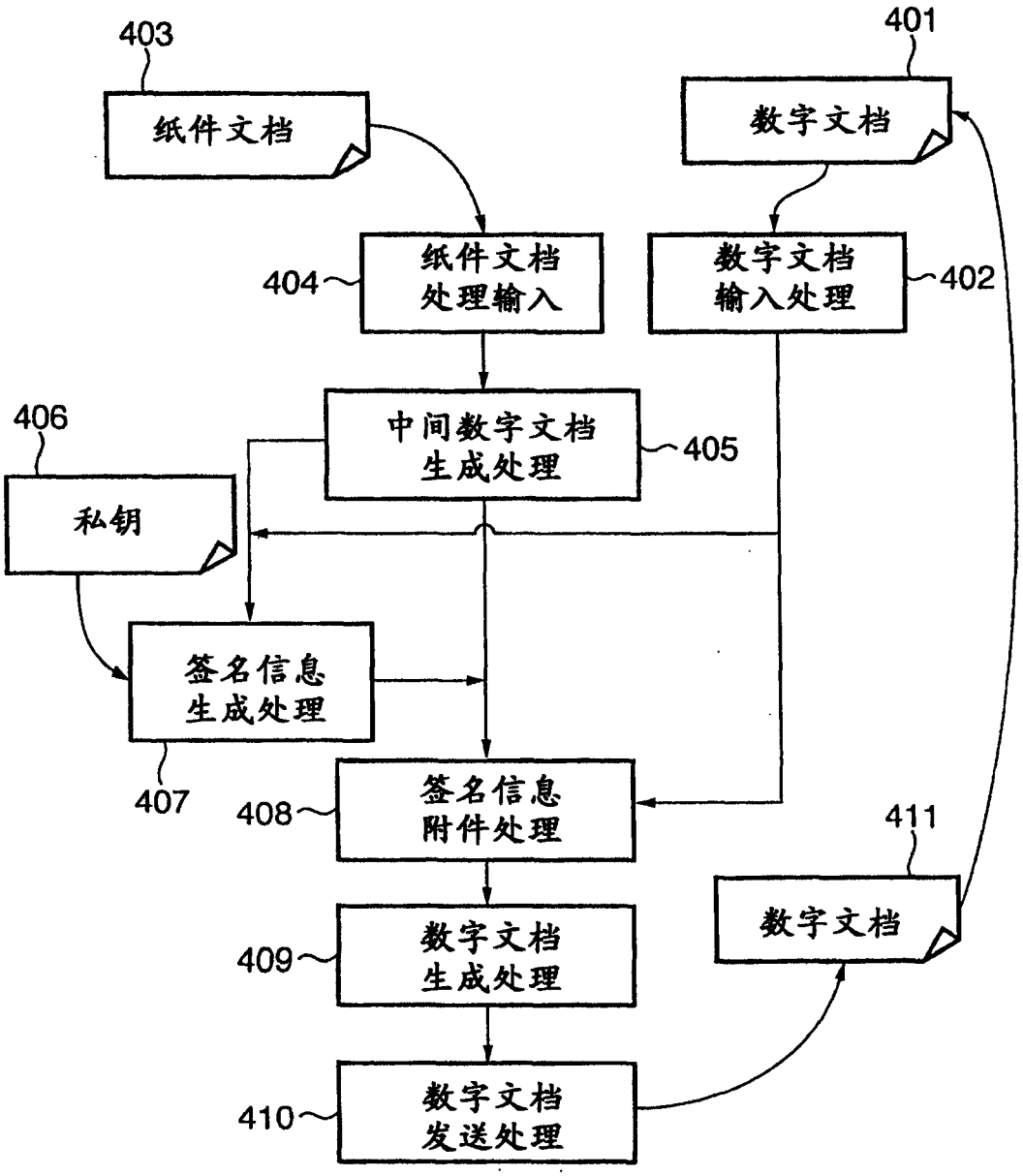

403
纸件文档
401
数字文档
404
纸件文档
处理输入
数字文档
输入处理
402
406
中间数字文档
生成处理
405
私钥
签名信息
生成处理
407
408
签名信息
附件处理
411
数字文档
409
数字文档
生成处理
410
数字文档
发送处理

图5

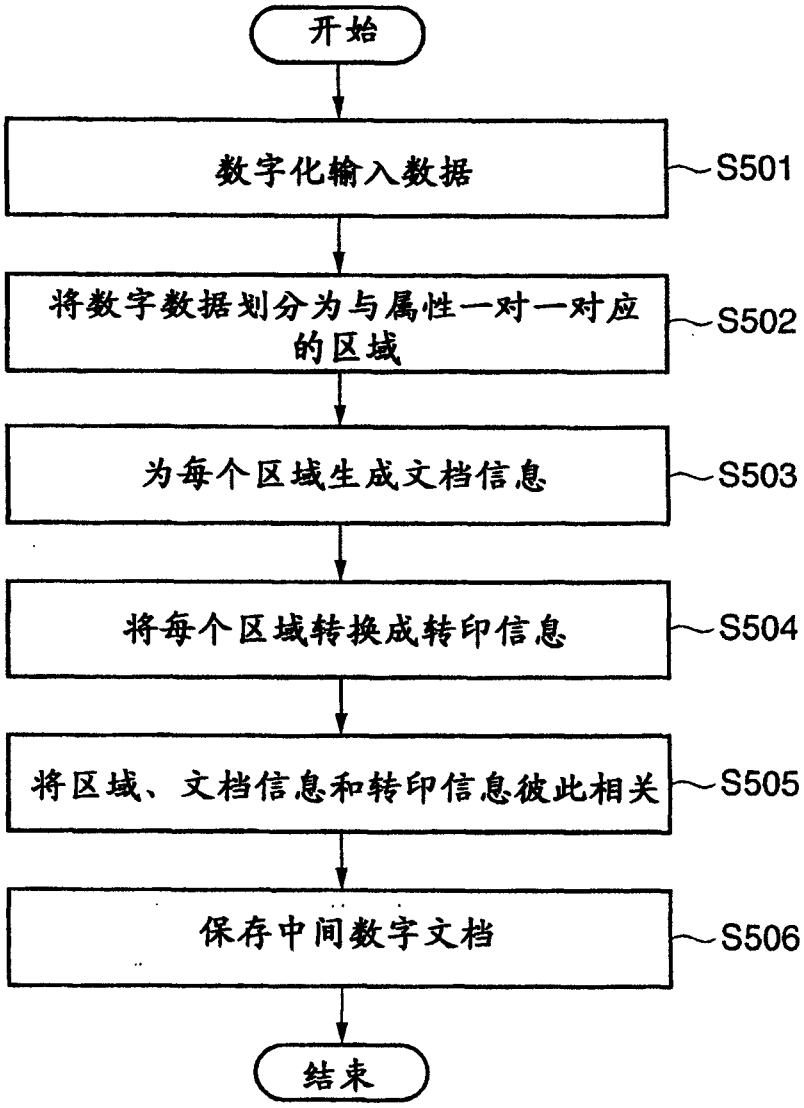

开始
数字化输入数据
S501
将数字数据划分为与属性一对一对应的区域
S502
为每个区域生成文档信息
S503
将每个区域转换成转印信息
S504
将区域、文档信息和转印信息彼此相关
S505
保存中间数字文档
S506
结束

图6A

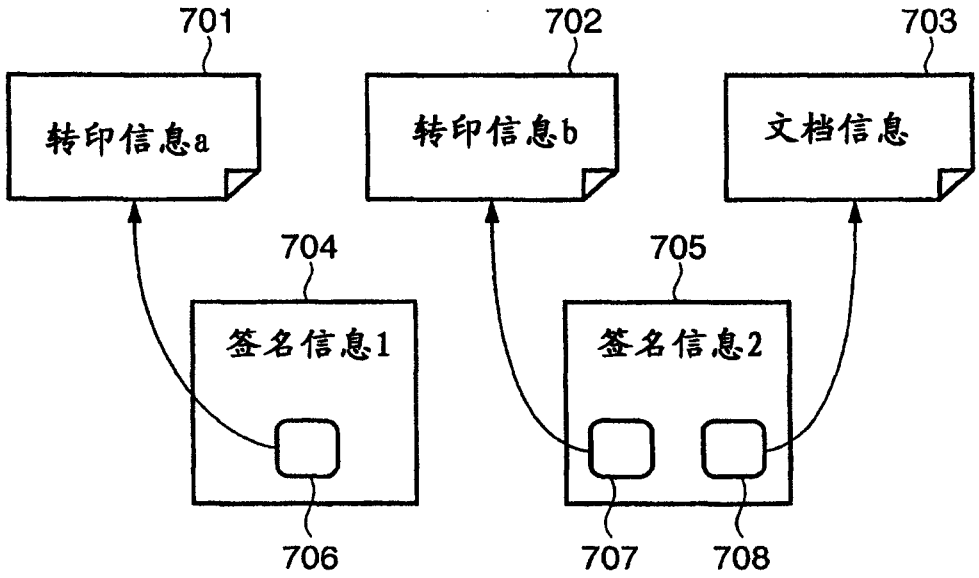

701
转印信息a
702
转印信息b
703
文档信息
704
签名信息1
705
签名信息2
706
707
708

图6B

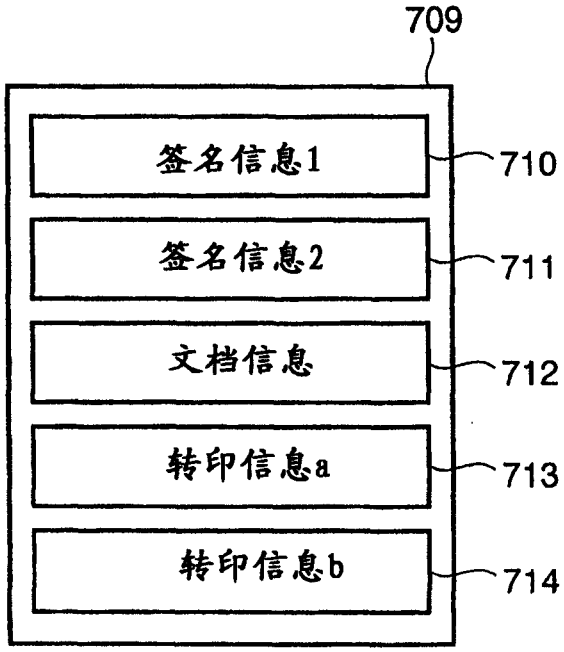

709
签名信息1
710
签名信息2
711
文档信息
712
转印信息a
713
转印信息b
714

图7

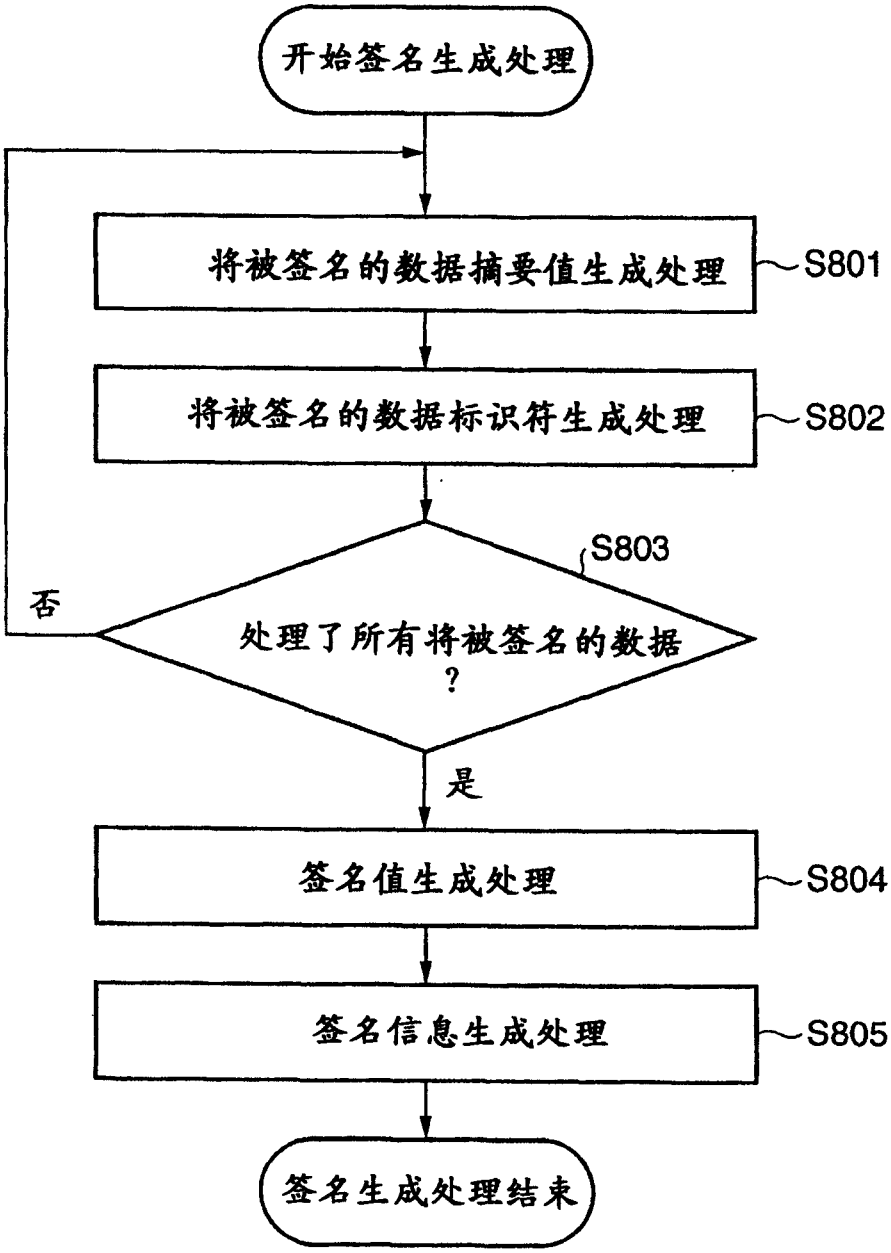

开始签名生成处理
将被签名的数据摘要值生成处理
S801
将被签名的数据标识符生成处理
S802
S803
处理了所有将被签名的数据？
否
是
签名值生成处理
S804
签名信息生成处理
S805
签名生成处理结束

图8

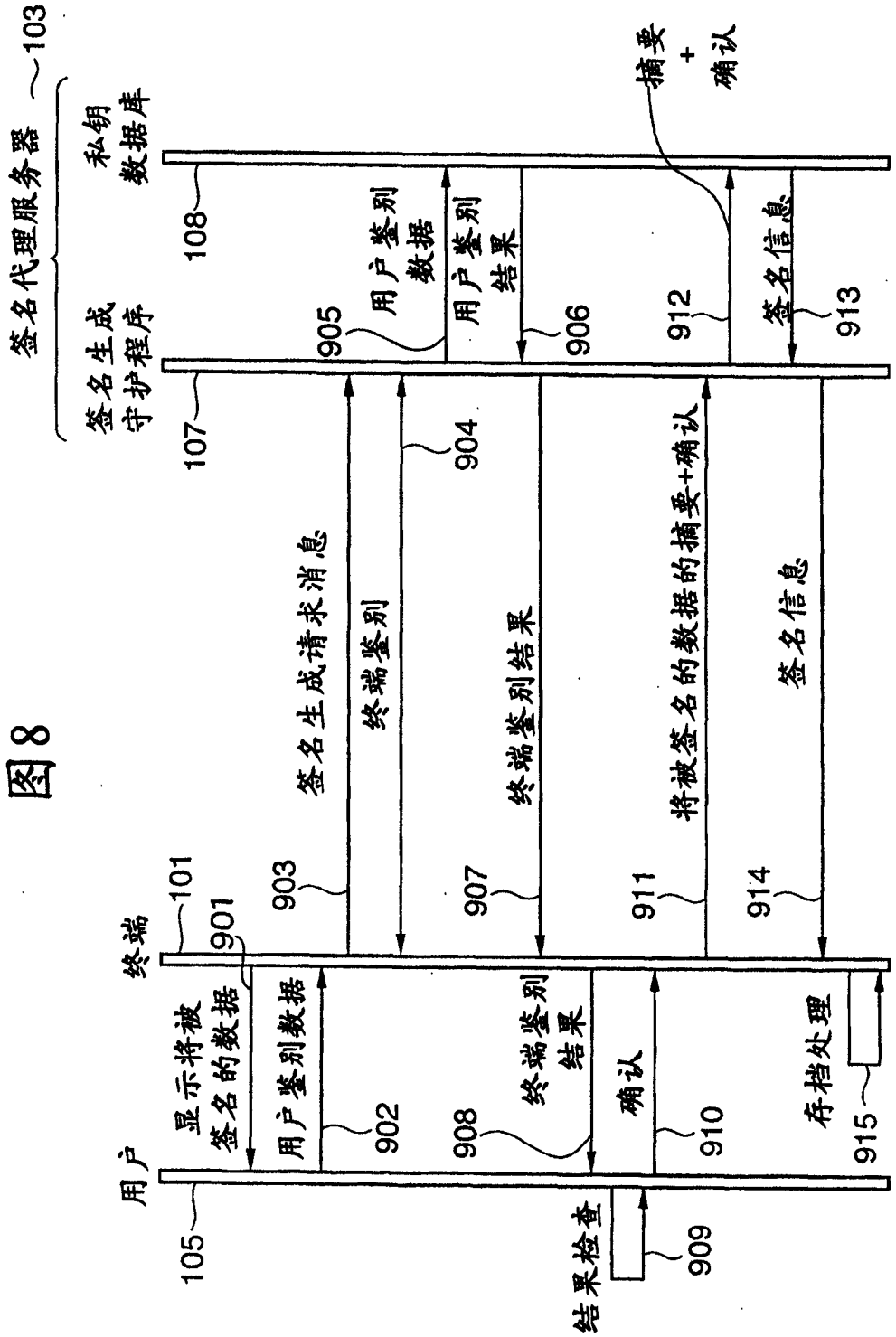

签名代理服务器 103
签名生成守护程序
私钥数据库
108
107
用户
终端
101
105
显示将被签名的数据
901
用户鉴别数据
902
903
签名生成请求消息
904
终端鉴别
905
用户鉴别数据
906
用户鉴别结果
907
终端鉴别结果
908
终端鉴别结果
909
结果检查
910
确认
911
将被签名的数据的摘要+确认
912
摘要+确认
913
签名信息
914
签名信息
915
存档处理

图9

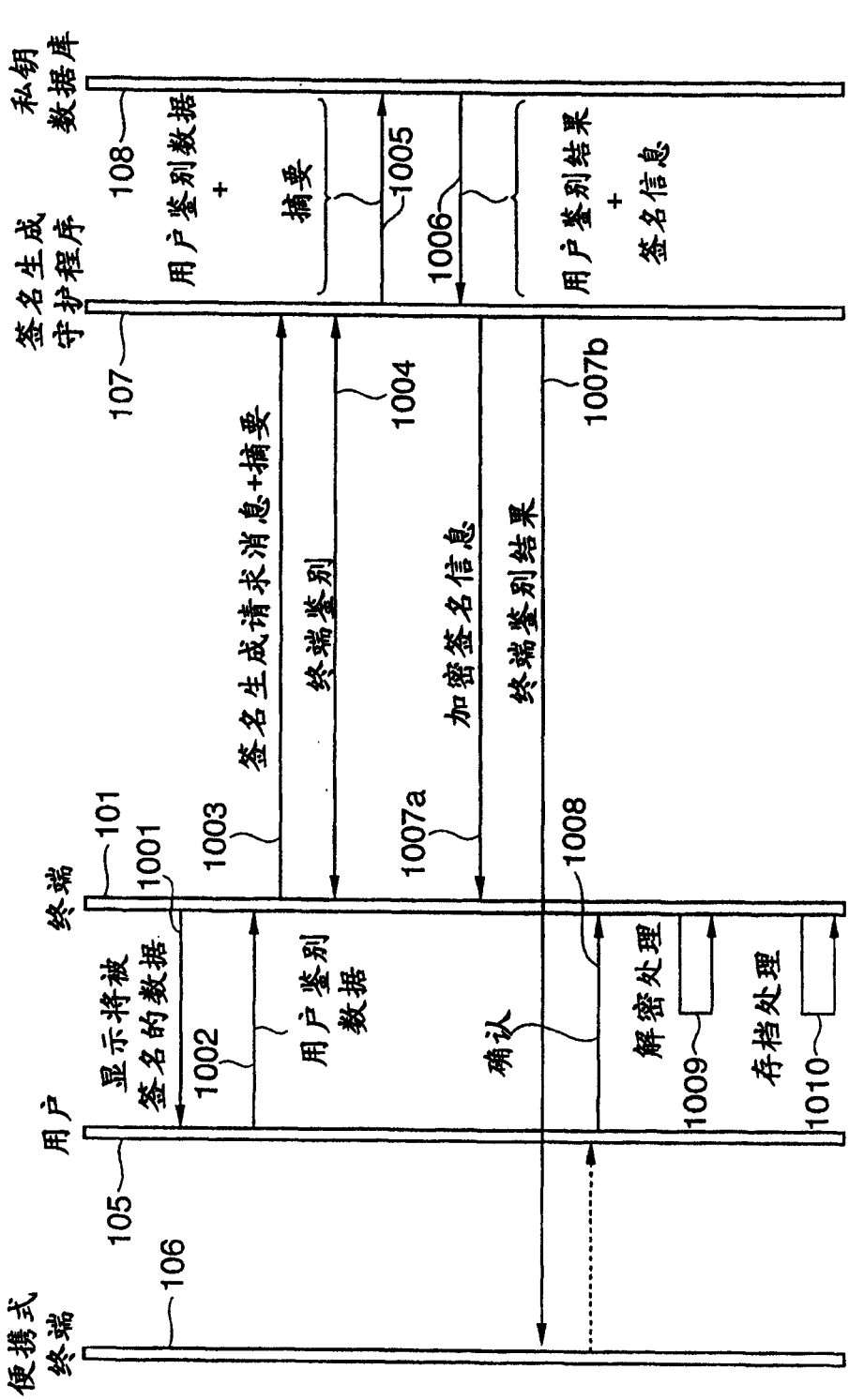

便携式终端
106
用户
105
显示将被签名的数据
1002
用户鉴别数据
确认
解密处理
1009
存档处理
1010
终端
101
1001
1003
签名生成请求消息+摘要
终端鉴别
1004
1007a
加密签名信息
终端鉴别结果
1008
1007b
签名代理服务器
103
签名生成守护程序
107
私钥数据库
108
用户鉴别数据
+
摘要
1005
1006
用户鉴别结果
+
签名信息

图10A

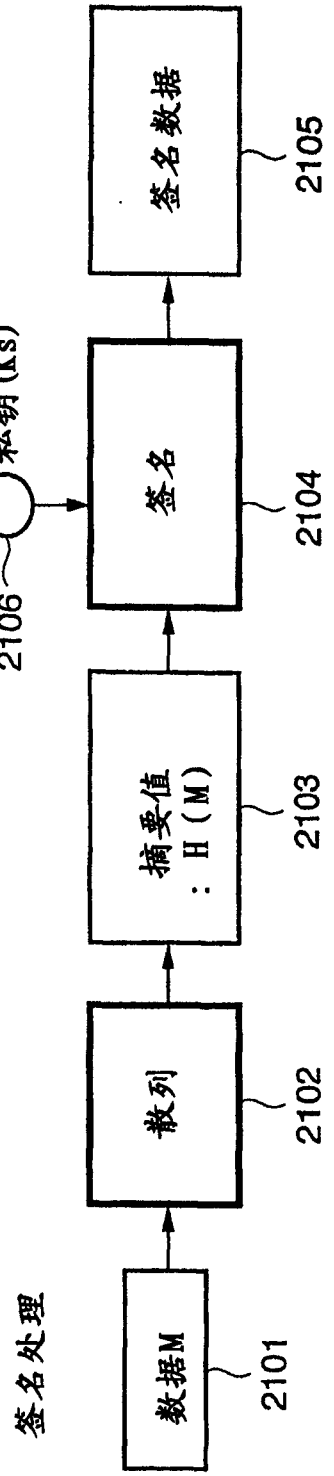

签名处理
数据M
2101
散列
2102
摘要值
：H（M）
2103
私钥（Ks）
2106
签名
2104
签名数据
2105

图10B

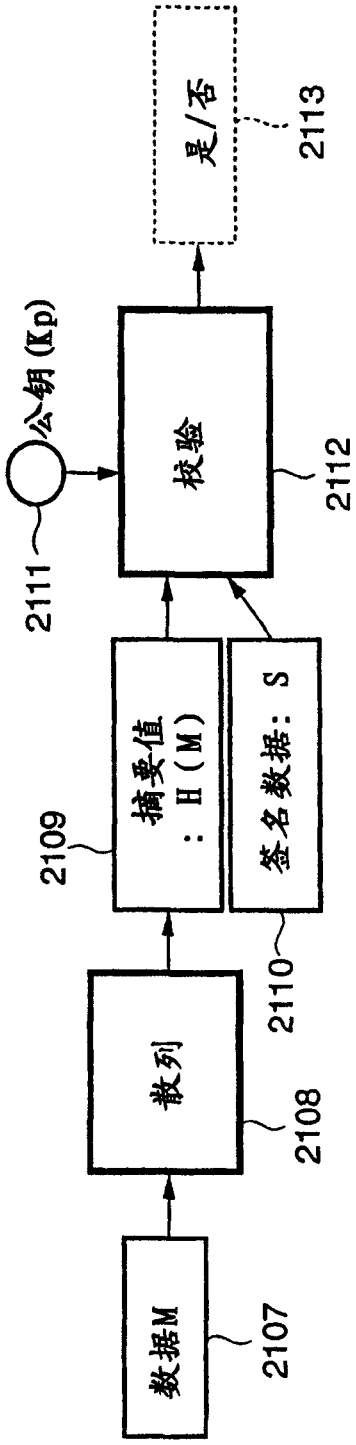
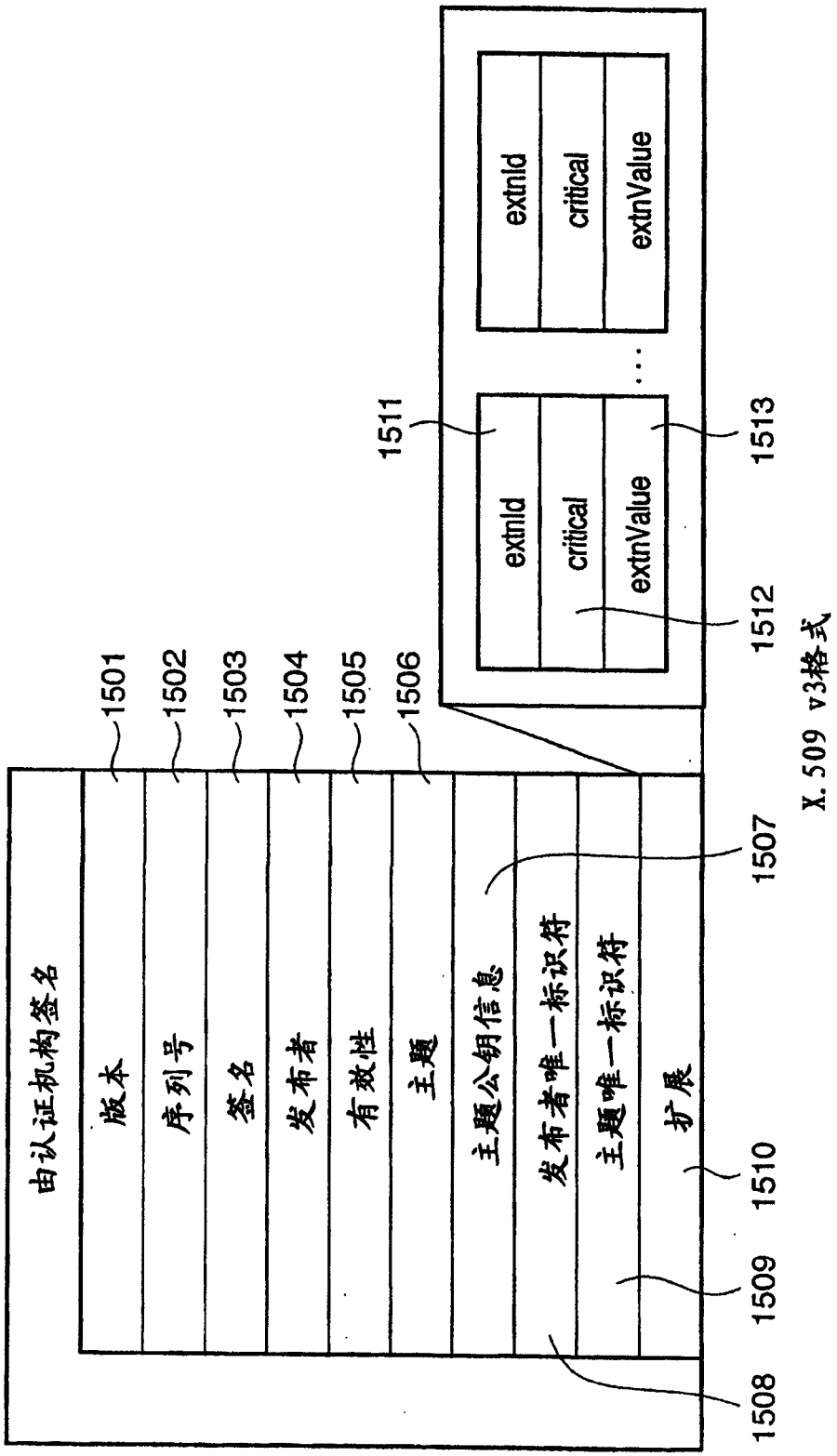

数据M
2107
散列
2108
摘要值
：H（M）
2109
签名数据：S
2110
公钥（Kp）
2111
校验
2112
是/否
2113

图 11


由认证机构签名
版本
序列号
签名
发布者
有效性
主题
主题公钥信息
发布者唯一标识符
主题唯一标识符
扩展
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
extnId
critical
extnValue
X.509 v3格式