(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1839581 B
(45)授权公告日 2011.03.30

(21)申请号 200480024038.7
(22)申请日 2004.06.30
(30)优先权数据
188139/2003 2003.06.30 JP
179562/2004 2004.06.17 JP
(85)PCT申请进入国家阶段日
2006.02.21
(86)PCT申请的申请数据
PCT/JP2004/009608 2004.06.30
(87)PCT申请的公布数据
WO2005/002133 JA 2005.01.06
(73)专利权人 索尼株式会社
地址 日本东京都
(72)发明人 胜部友浩 伊达秀树 佐藤敦司
杉田优 三浦贵之 小野刚
宫田耕自
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杨凯 王勇
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
(56)对比文件
JP 特开2003-110543 A,2003.04.11, 全文.
WO 00/62260 A1,2000.10.19, 全文.
JP 特开平6-244832 A,1994.09.02, 全文.
CN 1381016 A,2002.11.20, 全文.
JP 特开平8-125651 A,1996.05.17, 全文.
审查员 姚雅倩

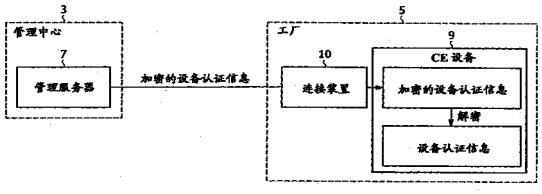
权利要求书 4 页 说明书 25 页 附图 18 页

(54)发明名称

装置认证信息安装系统

(57)摘要

CE设备(9)是一种能够在其中以高安全性包括设备认证信息的终端。管理服务器(7)将设备认证信息加密并将加密的设备认证信息传送到工厂(5)。工厂工人将连接装置(10)链接到CE设备(9)的连接器。由管理服务器(7)传送到工厂(5)的加密的设备认证信息经连接装置(10)以加密状态原样提供到CE设备(9)。CE设备(9)包括嵌入的写入模块,用于将加密的设备认证信息解密并将设备认证信息存储在存储单元中。也就是说,经连接装置(10)提供的设备认证信息由写入模块解密并存储在CE设备(9)中采用的存储单元中。由于设备认证信息以加密状态原样提供到CE设备(9),因此,设备认证信息可以高安全性存储在其中。



CN 1839581 B

1. 一种设备认证信息包括系统，它包括一个提供服务器和一个终端，并用于在所述终端中包括设备认证信息作为由设备认证服务器用于认证所述终端的信息；其中：

所述提供服务器提供源信息作为用于生成到所述终端的设备认证信息的源，并将所述设备认证信息或所述源信息提供给所述设备认证服务器用以认证所述设备；以及

所述终端通过使用所述接收的源信息，将信息存储为传送所述设备认证信息所需的信息，并在终端认证时通过使用所述存储信息，将从所述源信息生成的所述设备认证信息传送到所述设备认证服务器。

2. 如权利要求 1 所述的设备认证信息包括系统，其中：

所述提供服务器为所述终端提供一个转换值，该转换值是通过对从所述源信息生成的设备认证信息使用预定定向功能而执行的转换处理而获得的；

所述终端通过对从所述接收源信息生成的设备认证信息执行使用所述预定定向功能的转换处理而生成转换值；以及

所述终端比较所述生成的转换值与从所述提供服务器收到的所述转换值，以产生所述生成的转换值是否等于所述接收的转换值的确定结果。

3. 如权利要求 1 所述的设备认证信息包括系统，其中：

所述终端为所述提供服务器提供一个转换值，该转换值是通过对从所述源信息生成的设备认证信息使用预定定向功能而执行的转换处理而获得的；

所述提供服务器通过对从由所述终端接收的所述源信息而生成的设备认证信息执行使用所述预定定向功能的转换处理而生成转换值；以及

所述提供服务器比较所述生成的转换值与从所述终端收到的所述转换值，以产生所述生成的转换值是否等于所述接收的转换值的确定结果。

4. 一种用于安全地处理设备认证信息的终端，包括：

源信息获取装置，用于获取由提供服务器提供的、作为用于生成设备认证信息的源的源信息；

生成装置，用于从所述获取的源信息而生成设备认证信息；以及

设备认证信息传输装置，用于在设备认证时将所述生成的设备认证信息传送到设备认证服务器。

5. 如权利要求 4 所述的终端，其中：

所述源信息是作为将所述设备认证信息加密的处理结果而得到的加密设备认证信息；以及

所述生成装置通过将所述加密设备认证信息解密而生成所述设备认证信息。

6. 如权利要求 4 所述的终端，还包括存储装置，用于将所述生成装置生成的设备认证信息加密并存储加密所述设备认证信息的结果，其中，所述设备认证信息传输装置将存储在所述存储装置中的设备认证信息解密，并传送将所述设备认证信息解密的结果。

7. 如权利要求 6 所述的终端，还包括密钥生成装置，用于为处理生成加密密钥，所述处理将要存储在所述存储装置中的设备认证信息加密，并在需要利用所述加密密钥时，通过使用信息，将存储在所述存储装置中的设备认证信息解密。

8. 如权利要求 7 所述的终端，还包括密钥删除装置，用于在使用所述加密密钥后的预定时期内删除所述生成的加密密钥。

9. 如权利要求 4 所述的终端，还包括：

转换值获取装置，用于获取由于通过对来自所述提供服务器的所述设备认证信息使用预定单向功能而执行转换处理获得的转换值；

转换值计算装置，用于通过对所述生成的设备认证信息执行使用所述预定单向功能的转换处理来计算转换值；以及

确定装置，用于产生确定所述获取的转换值是否等于所述计算的转换值的结果。

10. 如权利要求 9 所述的终端，还包括：

转换值计算装置，用于通过对所述生成的设备认证信息执行使用另一预定单向功能的转换处理来计算另一转换值；以及

转换值提供装置，用于将所述另一计算的转换值提供给所述提供服务器。

11. 如权利要求 4 所述的终端，还包括：

转换值计算装置，用于通过对所述生成的设备认证信息执行使用预定单向功能的转换处理来计算转换值；以及

转换值提供装置，用于将所述计算的转换值提供给所述提供服务器。

12. 如权利要求 4 所述的终端，还包括用于存储所述获取的源信息的存储装置，其中，所述设备认证信息传输装置从所述存储的源信息生成设备认证信息，并将所述设备认证信息传送到所述设备认证服务器。

13. 一种在实施为计算机的终端中采用的设备认证信息处理方法，该终端包括源信息获取装置、生成装置和设备认证信息传输装置，所述设备认证信息处理方法包括：

源信息获取步骤，驱动所述源信息获取装置以获取由提供服务器提供的、作为用于生成设备认证信息的源的源信息；

生成步骤，驱动所述生成装置以从所述获取的源信息来生成设备认证信息；以及

设备认证信息传输步骤，驱动所述设备认证信息传输装置以在设备认证时将所述生成的设备认证信息传送到设备认证服务器。

14. 如权利要求 13 所述的设备认证信息处理方法，由此：

所述源信息为由于将所述设备认证信息加密的处理而获得的加密设备认证信息；以及

在所述生成步骤中，通过将所述加密的设备认证信息解密而生成所述设备认证信息。

15. 如权利要求 13 所述的设备认证信息处理方法，还包括存储步骤，将由所述生成装置生成的设备认证信息加密，并将加密所述设备认证信息的结果存储到也在所述计算机中采用的存储装置，由此，在所述设备认证信息传输步骤中，将存储在所述存储装置中的设备认证信息解密和传送。

16. 如权利要求 15 所述的设备认证信息处理方法，其中，所述计算机还包括密钥生成装置，所述设备认证信息处理方法还包括密钥生成步骤，驱动所述密钥生成装置以生成加密密钥，之后，在将要存储到所述存储装置的设备认证信息加密并通过使用信息将存储在所述存储装置中的设备认证信息解密的处理中使用所述加密密钥。

17. 如权利要求 16 所述的设备认证信息处理方法，其中，所述计算机还具有密钥删除装置，所述设备认证信息处理方法还包括密钥删除步骤，驱动所述密钥删除装置在所述加密密钥使用后预定时期内将所述生成的加密密钥删除。

18. 如权利要求 13 所述的设备认证信息处理方法，其中，所述计算机还包括转换值获

取装置、转换值计算装置和确定装置，所述设备认证信息处理方法还包括：

转换值获取步骤，驱动所述转换值获取装置以获取由于通过对来自所述提供服务器的所述设备认证信息使用预定单向功能而执行转换处理所获得的转换值；

转换值计算步骤，驱动所述转换值计算装置以通过对所述生成的设备认证信息执行使用所述预定单向功能的转换处理来计算转换值；以及

确定步骤，驱动所述确定装置以产生所述获取的转换值是否等于所述计算的转换值的确定结果。

19. 如权利要求 18 所述的设备认证信息处理方法，其中，所述计算机还包括转换值计算装置和转换值提供装置，所述设备认证信息处理方法还包括：

转换值计算步骤，驱动所述转换值计算装置以通过对所述生成的设备认证信息执行使用另一单向功能的转换处理来计算另一转换值；以及

转换值提供步骤，驱动所述转换值提供装置以将所述另一计算的转换值提供给所述提供服务器。

20. 如权利要求 13 所述的设备认证信息处理方法，其中，所述计算机还包括转换值计算装置和转换值提供装置，所述设备认证信息处理方法还包括：

转换值计算步骤，驱动所述转换值计算装置以通过对所述生成的设备认证信息执行使用预定单向功能的转换处理来计算转换值；以及

转换值提供步骤，驱动所述转换值提供装置以将所述计算的转换值提供给所述提供服务器。

21. 如权利要求 13 所述的设备认证信息处理方法，其中，所述计算机还包括用于存储所述获取的源信息的存储装置，并且在所述设备认证信息传输步骤中，设备认证信息从所述存储的源信息生成并传送到所述设备认证服务器。

22. 一种提供服务器，包括：

源信息提供装置，用于为终端提供作为用于生成设备认证信息的源的源信息；

设备认证信息提供装置，用于将所述设备认证信息或所述源信息提供给设备认证服务器用以认证所述终端；

转换值获取装置，用于获取由于通过对依据来自所述终端的接收的源信息而生成的设备认证信息使用预定单向功能而执行转换处理所获得的转换值；

转换值计算装置，用于通过对所述设备认证信息执行使用所述单向功能的转换处理来计算转换值；以及

确定装置，用于产生所述获取的转换值是否等于所述计算的转换值的确定结果。

23. 如权利要求 22 所述的提供服务器，还包括确定结果传输装置，用于将所述确定装置产生的确定结果传送到主要组织用以包括所述源信息。

24. 一种在计算机中采用的设备认证信息提供方法，所述计算机包括源信息提供装置、设备认证信息提供装置、转换值获取装置、转换值计算装置及确定装置，以执行：

源信息提供步骤，驱动所述源信息提供装置用以为终端提供用作生成设备认证信息的源的源信息；

设备认证信息提供步骤，驱动所述设备认证信息提供装置用以将所述设备认证信息或所述源信息提供给设备认证服务器用以认证所述终端；

转换值获取步骤，驱动所述转换值获取装置，用以获取由于通过对依据来自所述终端的所述接收的源信息所生成的设备认证信息使用预定单向功能而执行的转换处理获得的转换值；

转换值计算步骤，驱动所述转换值计算装置以通过对所述设备认证信息执行使用所述单向功能的转换处理来计算转换值；以及

确定步骤，驱动所述确定装置以产生所述获取的转换值是否等于所述计算的转换值的确定结果。

25. 如权利要求 24 所述的设备认证信息提供方法，包括确定结果传输步骤，驱动在所述计算机中做为另外装置而额外采用的确定结果传输装置，用于将所述确定装置产生的确定结果传送到主要组织用以包括所述源信息。

装置认证信息安装系统

技术领域

[0001] 本发明涉及诸如终端等设备。更具体地说，本发明涉及一种通过将设备认证信息加密，在设备中存储所述加密信息并在所述设备中将所述加密信息解密的方式，在所述设备中安全处理所述信息的技术。

背景技术

[0002] 近年来，CE（消费类电子产品）设备变得普遍并得到广泛地使用。CE 设备的示例有诸如录像机、立体音响和电视等视听设备和诸如电饭煲和冰箱等家用电子器材及其它电子设备，每个设备包括了嵌入式计算机以从通过网络提供的服务获益。

[0003] 由服务器提供的服务包括需要认证 CE 设备的服务。为此，CE 设备包括预先在工厂嵌入的设备认证信息，做为用于认证设备的信息。

[0004] 图 18 是在设备中包括设备认证信息的常规方法说明中参照的说明图。要包括在 CE 设备中的设备认证信息由管理中心 103 的管理服务器 107 管理。

[0005] 管理服务器 107 将设备认证信息传送到工厂 105，该工厂做为制造 CE 设备的工厂。

[0006] 由于设备认证信息是必须严格保密处理的秘密信息，因此，设备认证信息传送到工厂 105 时要尽力防止信息泄漏给他人。

[0007] 在工厂 105，连接装置 110 链接到 CE 设备 109 的连接器。连接装置 110 是用于从管理服务器 107 接收设备认证信息并将信息提供到 CE 设备 109 的装置。

[0008] 连接装置 110 具有一个嵌入功能把加密的装置认证信息解密。这样，连接装置 110 能够对从管理服务器 107 接收的加密的设备认证信息进行解密。

[0009] 连接装置 110 随后将解密的设备认证信息提供到 CE 设备 109 以存储在 CE 设备 109 中采用的存储单元中。

[0010] 做为如上所述将设备认证信息包括在 CE 设备中的一个发明，在日本公开特许公报（未审查）2001-134654 中公开了发现的一种电子设备制造系统和电子设备制造方法。

[0011] 根据此发明，基于贴在在 CE 设备上的条形码标签印记上所写的产品序列号，从数据库中读出设备的设备认证信息并包括在设备中。

[0012] 附带提到的是，通过常规方法，连接装置 110 将设备认证信息解密。因此，设备认证信息很可能从连接装置 110 泄漏。

[0013] 特别是在近年来，有许多情况是委托低成本的海外生产商制造产品。因此，必需提供一种机制，以高可靠性将传送到工厂 105 的设备认证信息包括在 CE 设备 109 中而不会向他人泄漏设备认证信息。

[0014] 提供一种能够将设备认证信息包括在具有高安全性的设备中的终端或诸如此类，这是人们所期望的。

[0015] 以严格的置信度处理信息的状态，确认设备认证信息已正确包括在设备中，这是人们所希望的。

发明内容

[0016] 为实现本发明的上述目的，根据本发明的配置 1，提供了一种设备认证信息包括系统，它包括一个提供服务器和一个终端，并用于在所述终端中包括设备认证信息以做为由设备认证服务器用于认证所述终端的信息。设备认证信息包括系统的特征在于：

[0017] 所述提供服务器提供源信息，做为生成到所述终端的设备认证信息的源，并提供所述设备认证信息或所述源信息到所述设备认证服务器以认证所述终端；以及

[0018] 所述终端通过使用所述接收的源信息，将信息存储为传送所述设备认证信息所必需的信息，并在终端认证时通过使用所述存储信息，将从所述源信息生成的设备认证信息传送到所述设备认证服务器。

[0019] 根据配置 2，在如配置 1 所述的设备认证信息包括系统中，

[0020] 所述提供服务器为所述终端提供一个转换值，该值是通过在从所述源信息生成的设备认证信息上使用预定定向功能而执行的转换处理获得；

[0021] 所述终端通过在从所述接收源信息生成的设备认证信息上执行使用所述预定定向功能的转换处理而生成转换值；以及

[0022] 所述终端比较所述生成的转换值与从所述提供服务器收到的所述转换值，产生所述生成的转换值是否等于所述接收的转换值的确定结果。

[0023] 根据配置 3，在如配置 1 所述的设备认证信息包括系统中，

[0024] 所述终端为所述提供服务器提供一个转换值，该值是通过在从所述源信息生成的设备认证信息上使用预定定向功能而执行的转换处理获得；

[0025] 所述提供服务器通过在从所述接收源信息生成的设备认证信息上执行使用所述预定定向功能的转换处理而生成转换值；以及

[0026] 所述提供服务器比较所述生成的转换值与从所述终端收到的所述转换值，产生所述生成的转换值是否等于所述接收的转换值的确定结果。

[0027] 为实现本发明的上述目的，根据本发明的配置 4，提供了一种终端，其特征在于所述终端包括：

[0028] 源信息获取装置，获取由提供服务器提供、作为用于生成设备认证信息的源的源信息；

[0029] 生成装置，从所述获取的源信息生成设备认证信息；以及

[0030] 设备认证信息传输装置，在设备认证时将所述生成的设备认证信息传送到设备认证服务器。

[0031] 根据配置 5，在如配置 4 所述的终端中，

[0032] 所述源信息是由于将所述设备认证信息加密的处理而得到的加密设备认证信息；以及

[0033] 所述生成装置通过将所述加密设备认证信息解密而生成所述设备认证信息。

[0034] 根据配置 6，如配置 4 所述的终端还具有存储装置，用于将所述生成装置生成的设备认证信息加密并存储加密所述设备认证信息的结果，其中，所述设备认证信息传输装置将存储在所述存储装置中的设备认证信息解密，并传送将所述设备认证信息解密的结果。

[0035] 根据配置 7，如配置 6 所述的终端还具有密钥生成装置，用于为处理生成加密密钥，用于以下处理：加密要存储在所述存储装置中的设备认证信息，并在需要利用所述加密

密钥时，通过使用所述终端特有的信息，将存储在所述存储装置中的设备认证信息解密。

[0036] 根据配置 8，如配置 7 所述的终端还具有密钥删除装置，用于在使用所述加密密钥后预定时期内删除所述生成的加密密钥。

[0037] 根据配置 9，如配置 4 所述的终端还具有：

[0038] 转换值获取装置，用于获取由于通过在从所述提供服务器来的设备认证信息上使用预定单向功能而执行转换处理获得的转换值；

[0039] 转换值计算装置，用于通过在所述生成的设备认证信息上使用所述预定单向功能执行转换处理，计算转换值；以及

[0040] 确定装置，用于产生所述获取的转换值是否等于所述计算出的转换值的确定结果。

[0041] 根据配置 10，如配置 9 所述的终端还具有：

[0042] 转换值计算装置，用于通过在所述生成的设备认证信息上使用另一预定单向功能执行转换处理，计算转换值；以及

[0043] 转换值提供装置，用于将所述计算出的转换值提供到所述提供服务器。

[0044] 根据配置 11，如配置 4 所述的终端还具有：

[0045] 转换值计算装置，用于通过在所述生成的设备认证信息上使用预定单向功能执行转换处理，计算转换值；以及

[0046] 转换值提供装置，用于将所述计算出的转换值提供到所述提供服务器。

[0047] 根据配置 12，如配置 4 所述的终端还具有用于存储所述获取的源信息的存储装置，其中，所述设备认证信息传输装置从所述存储的源信息生成设备认证信息，并将所述设备认证信息传送到所述设备认证服务器。

[0048] 为实现本发明的上述目的，根据本发明的配置 13，提供了在实施为计算机的终端中采用的一种设备认证信息处理方法，该终端包括源信息获取装置、生成装置和设备认证信息传输装置。所述设备认证信息处理方法的特征在于所述设备认证信息方法具有：

[0049] 源信息获取步骤，驱动所述源信息获取装置获取由提供服务器提供、作为生成设备认证信息的源的源信息；

[0050] 生成步骤，驱动所述生成装置从所述获取的源信息生成设备认证信息；以及

[0051] 设备认证信息传输步骤，驱动所述设备认证信息传输装置在设备认证时将所述生成的设备认证信息传送到设备认证服务器。

[0052] 根据配置 14，通过如配置 13 所述的设备认证信息处理方法，

[0053] 所述源信息为由于将所述设备认证信息加密的处理而获得的加密设备认证信息；以及

[0054] 在所述生成步骤中，通过将所述加密的设备认证信息解密而生成所述设备认证信息。

[0055] 根据配置 15，如配置 13 所述的设备认证信息处理方法还具有存储步骤，将由所述生成装置生成的设备认证信息加密，并将加密所述设备认证信息的结果存储到也在所述计算机中采用的存储装置，由此，在所述设备认证信息传输步骤中，将存储在所述存储装置中的设备认证信息解密和传送。

[0056] 根据配置 16，采用如配置 15 所述的设备认证信息处理方法的计算机还具有密钥

生成装置，并且所述设备认证信息处理方法还具有驱动所述密钥生成装置以生成加密密钥的密钥生成步骤，之后，在将要存储到所述存储装置的设备认证信息加密并通过使用所述终端特有的信息将存储在所述存储装置中的设备认证信息解密的处理中使用所述加密密钥。

[0057] 根据配置 17，采用如配置 16 所述的设备认证信息处理方法的计算机还具有密钥删除装置，并且所述设备认证信息处理方法还具有密钥删除步骤，驱动所述密钥删除装置在所述加密密钥使用后预定时期内将所述生成的加密密钥删除。

[0058] 根据配置 18，采用如配置 13 所述设备认证信息处理方法的计算机还具有转换值获取装置、转换值计算装置和确定装置，并且所述设备认证信息处理方法还包括：

[0059] 转换值获取步骤，驱动所述转换值获取装置获取由于通过在从所述提供服务器来的设备认证信息上使用预定单向功能而执行转换处理获得的转换值；

[0060] 转换值计算步骤，驱动所述转换值计算装置通过在所述生成的设备认证信息上使用所述预定单向功能执行转换处理，计算转换值；以及

[0061] 确定步骤，驱动所述确定装置产生所述获取的转换值是否等于所述计算出的转换值的确定结果。

[0062] 根据配置 19，采用如配置 18 所述设备认证信息处理方法的计算机还具有转换值计算装置和转换值提供装置，并且所述设备认证信息处理方法还包括：

[0063] 转换值计算步骤，驱动所述转换值计算装置通过在所述生成的设备认证信息上使用另一单向功能执行转换处理，计算转换值；以及

[0064] 转换值提供步骤，驱动所述转换值提供装置将所述计算出的转换值提供到所述提供服务器。

[0065] 根据配置 20，采用如配置 13 所述设备认证信息处理方法的计算机还具有转换值计算装置和转换值提供装置，并且所述设备认证信息处理方法还包括：

[0066] 转换值计算步骤，驱动所述转换值计算装置通过在所述生成的设备认证信息上使用预定单向功能执行转换处理，计算转换值；以及

[0067] 转换值提供步骤，驱动所述转换值提供装置将所述计算出的转换值提供到所述提供服务器。

[0068] 根据配置 21，采用如配置 13 所述设备认证信息处理方法的计算机还具有用于存储所述获取的源信息的存储装置，并且在所述设备认证信息传输步骤中，设备认证信息从所述存储的源信息生成并传送到所述设备认证服务器。

[0069] 为实现本发明的上述目的，根据本发明的配置 22，提供了一种由计算机执行的设备认证信息处理程序。所述设备认证信息处理程序的特征在于所述设备认证信息处理程序包括：

[0070] 源信息获取功能，获取由提供服务器提供、做为生成设备认证信息的源的源信息；

[0071] 生成功能，从所述获取的源信息生成设备认证信息；以及

[0072] 设备认证信息传输功能，在设备认证时将所述生成的设备认证信息传送到设备认证服务器。

[0073] 根据配置 23，在采用如配置 22 所述的设备认证信息处理程序中，所述源信息是由

于将所述设备认证信息加密的处理而得到的加密设备认证信息，并且所述生成功能通过将所述加密设备认证信息解密而生成所述设备认证信息。

[0074] 根据配置 24，如配置 22 所述的设备认证信息处理程序还具有存储功能，将所述生成功能生成的设备认证信息加密并存储加密所述设备认证信息的结果，其中，所述设备认证信息传输功能将由所述存储功能存储的设备认证信息解密，并传送将所述设备认证信息解密后的结果。

[0075] 根据配置 25，如配置 24 所述的设备认证信息处理程序还具有密钥生成功能，该功能由所述计算机执行以生成加密密钥，用于以下处理：将要由所述存储功能存储的设备认证信息加密，并在需要利用所需加密密钥时，通过使用所述终端特有的信息，将所述存储功能存储的设备认证信息解密。

[0076] 根据配置 26，如配置 25 所述的设备认证信息处理程序还具有由所述计算机执行、在使用所述加密密钥后预定时期内删除所述生成的加密密钥的密钥删除功能。

[0077] 根据配置 27，如配置 22 所述的设备认证信息处理程序还具有：

[0078] 转换值获取功能，由所述计算机执行，获取由于通过在从所述提供服务器来的设备认证信息上使用预定单向功能而执行转换处理获得的转换值；

[0079] 转换值计算功能，由所述计算机执行，通过在所述生成的设备认证信息上使用所述预定单向功能执行转换处理，计算转换值；以及

[0080] 确定功能，由所述计算机执行，产生所述获取的转换值是否等于所述计算出的转换值的确定结果。

[0081] 根据配置 28，如配置 27 所述的设备认证信息处理程序还具有：

[0082] 转换值计算功能，由所述计算机执行，通过在所述生成的设备认证信息上使用另一单向功能执行转换处理，计算转换值；以及

[0083] 转换值提供功能，由所述计算机执行，将所述计算出的转换值提供到所述提供服务器。

[0084] 根据配置 29，如配置 22 所述的设备认证信息处理程序还具有：

[0085] 转换值计算功能，由所述计算机执行，通过在所述生成的设备认证信息上使用预定单向功能执行转换处理，计算转换值；以及

[0086] 转换值提供功能，由所述计算机执行，将所述计算出的转换值提供到所述提供服务器。

[0087] 根据配置 30，如配置 22 所述的设备认证信息处理程序还具有由所述计算机执行以存储所述获取的源信息的存储功能，其中，所述设备认证信息传输功能从所述存储的源信息生成设备认证信息并将设备认证信息传送到所述设备认证服务器。

[0088] 为实现本发明的上述目的，根据本发明的配置 31，提供了一种存储媒体，它可由计算机读取并用于存储由所述计算机执行以实施以下功能的设备认证信息处理程序：

[0089] 源信息获取功能，获取由提供服务器提供、作为生成设备认证信息的源的源信息；

[0090] 生成功能，从所述获取的源信息生成设备认证信息；以及

[0091] 设备认证信息传输功能，在设备认证时将所述生成的设备认证信息传送到设备认证服务器。

[0092] 为实现本发明的上述目的，根据本发明的配置 32，提供了一种提供服务器，其特征在于所述提供服务器包括：

[0093] 源信息提供装置，用于为终端提供作为生成设备认证信息的源的源信息；

[0094] 设备认证信息提供装置，用于将所述设备认证信息或源信息提供到设备认证服务器以认证的所述终端；

[0095] 转换值获取装置，用于获取由于通过在依据所述终端来的所述源信息生成的设备认证信息上使用预定单向功能而执行转换处理获得的转换值；

[0096] 转换值计算装置，用于通过在所述设备认证信息上使用所述单向功能执行转换处理，计算转换值；以及

[0097] 确定装置，用于产生所述获取的转换值是否等于所述计算出的转换值的确定结果。

[0098] 根据配置 33，如配置 32 所述的提供服务器还具有确定结果传输装置，用于将所述确定装置产生的确定结果传送到主要组织以包括所述源信息。

[0099] 为实现本发明的上述目的，根据本发明的配置 34，提供了一种在计算机中采用的设备认证信息提供方法，所述计算机包括源信息提供装置、设备认证信息提供装置、转换值获取装置、转换值计算装置及确定装置。所述设备认证信息提供方法的特征在于所述设备认证信息提供方法包括：

[0100] 源信息提供步骤，驱动所述源信息提供装置为终端提供做为生成设备认证信息的源的源信息；

[0101] 设备认证信息提供步骤，驱动所述设备认证信息提供装置将所述设备认证信息或所述源信息提供到设备认证服务器以认证所述终端；

[0102] 转换值获取步骤，驱动所述转换值获取装置，获取由于通过在依据从所述终端来的所述源信息生成的设备认证信息上使用预定单向功能而执行转换处理获得的转换值；

[0103] 转换值计算步骤，驱动所述转换值计算装置通过在所述设备认证信息上使用所述预定单向功能执行转换处理，计算转换值；以及

[0104] 确定步骤，驱动所述确定装置产生所述获取的转换值是否等于所述计算出的转换值的确定结果。

[0105] 根据配置 35，如配置 34 所述的设备认证信息提供方法还具有确定结果传输步骤，驱动在所述计算机中作为又一装置而另外采用的确定结果传输装置，用于将所述确定装置产生的确定结果传送到主要组织以包括所述源信息。

[0106] 为实现本发明的上述目的，根据本发明的配置 36，提供了一种由计算机执行以实施以下功能的设备认证信息提供程序：

[0107] 源信息提供功能，为终端提供用作生成设备认证信息的源的源信息；

[0108] 设备认证信息提供功能，将所述设备认证信息或源信息提供到设备认证服务器以认证的所述终端；

[0109] 转换值获取功能，获取由于在依据所述终端来的所述源信息生成的设备认证信息上使用预定单向功能而执行转换处理获得的转换值；

[0110] 转换值计算功能，通过在所述设备认证信息上使用所述单向功能执行转换处理，计算转换值；以及

[0111] 确定功能，产生所述获取的转换值是否等于所述计算出的转换值的确定结果。

[0112] 根据配置 37，如配置 36 所述的设备认证信息提供程序还具有由所述计算机执行的确定结果传输功能，以将所述确定功能产生的确定结果传送到主要组织以包括所述源信息。

[0113] 为实现本发明的上述目的，根据本发明的配置 38，提供了一种存储媒体，它可由计算机读取并用于存储由所述计算机执行以实施以下功能的设备认证信息处理程序：

[0114] 源信息提供功能，为终端提供用作生成设备认证信息的源的源信息；

[0115] 设备认证信息提供功能，将所述设备认证信息或源信息提供到设备认证服务器以认证的所述终端；

[0116] 转换值获取功能，获取由于通过在依据所述终端来的所述源信息生成的设备认证信息上使用预定单向功能而执行转换处理获得的转换值；

[0117] 转换值计算功能，通过在所述设备认证信息上使用所述单向功能执行转换处理，计算转换值；以及

[0118] 确定功能，产生所述获取的转换值是否等于所述计算出的转换值的确定结果。

[0119] 根据本发明，设备认证信息可包括在具有高安全性的设备中。另外，也可验证设备认证信息已正确包括在设备中，设备认证信息以保密状态原样保持。

附图说明

[0120] 图 1 是简单显示第一实施例的示范图；

[0121] 图 2 显示了第一实施例中制造 / 认证系统的典型配置；

[0122] 图 3 显示了根据第一实施例的设备认证部分的典型配置；

[0123] 图 4 显示了第一实施例中包括设备认证信息的准备阶段执行的工作过程解释中参照的流程图；

[0124] 图 5 显示了第一实施例中将设备认证信息包括到 CE 设备的过程解释中参照的流程图；

[0125] 图 6 显示了第一实施例中验证设备认证信息已正确包括到 CE 设备的过程解释中参照的流程图；

[0126] 图 7 显示了第一实施例中由设备认证服务器用做认证 CE 设备的过程的过程解释中参照的流程图；

[0127] 图 8 是示范图，显示了根据第一实施例在诸如设备认证服务器等设备中存储的表；

[0128] 图 9 显示了根据第一实施例的 CD 设备典型硬件配置；

[0129] 图 10 是简单显示第二实施例的示范图；

[0130] 图 11 显示了第二实施例中将设备认证信息包括到 CE 设备的过程解释中参照的流程图；

[0131] 图 12 显示了第二实施例中验证设备认证信息已正确包括到 CE 设备的过程解释中参照的流程图；

[0132] 图 13 显示了第二实施例中由设备认证服务器用做认证 CE 设备的过程的过程解释中参照的流程图；

[0133] 图 14 是示范图，显示了根据第二实施例在诸如设备认证服务器等设备中存储的表；

[0134] 图 15 显示了第三实施例中更新包括密钥的应用程序的过程解释中参照的流程图；

[0135] 图 16 显示了根据第四实施例的设备认证部分的典型配置；

[0136] 图 17 显示了第四实施例中验证设备认证信息正确包括到 CE 设备的过程解释中参照的流程图；以及

[0137] 图 18 是示范图，显示了包括认证信息的常规方法。

具体实施方式

[0138] 本发明的优选实施例将参照附图详细描述如下。

[0139] [第一实施例概述]

[0140] 图 1 是简单显示第一实施例的示范图。

[0141] 管理设备认证信息的管理服务器 7 安装在管理中心 3，并用于在将加密的设备认证信息传输到工厂 5 前将设备认证信息加密。

[0142] 连接装置 10 由工厂的工人链接到 CE 设备 9 的连接器。连接装置 10 将从管理服务器 7 收到的设备认证信息以其加密状态原样提供到 CE 设备 9。

[0143] CE 设备 9 包括嵌入式写入模块，用于将加密的设备认证信息解密，并在存储单元中存储解密结果。

[0144] 如上所述，写入模块将从连接装置 10 收到的加密设备认证信息解密，并将解密结果存储到 CE 设备 9 中嵌入的存储单元。

[0145] 连接装置 10 不同于常规系统中使用的连接装置 110，不同之处在于连接装置 10 不将从管理服务器 7 收到的设备认证信息解密，而是立刻原样将信息提供到 CE 设备 9。

[0146] 如上所述，在此实施例中，从也称为提供服务器的管理服务器 7 收到的设备认证信息由于要在 CE 设备 9 中解密，因而以加密状态提供到也称为终端的 CE 设备 9。因此，在包括设备认证信息的工作中，可提高设备认证信息的安全。

[0147] 要注意的是，上述说明只解释了实施例的基本概念。因此，对所述内容可进行多种改变。

[0148] 例如，如下面实施例说明中详细解释的一样，解密的设备认证信息可使用另一加密密钥再次加密，并存储在存储单元中以便进一步提高信息的安全。

[0149] 另外，工厂 5 和管理中心 3 各包括验证设备认证信息已包括在 CE 设备 9 的装置。

[0150] [第一实施例详情]

[0151] 图 2 显示了 CE 设备制造 / 认证系统 1 的典型配置。制造 / 认证系统 1 是用于制造和认证 CE 设备 9 的系统。图形既未显示向 CE 设备 9 提供服务的服务服务器，也未显示其它设备。

[0152] 制造 / 认证系统 1 包括业务组织 11、管理中心 3、工厂 5、CE 设备 9 及设备认证服务器 8。

[0153] 业务组织 11 是制造 CE 设备 9 的公司。业务组织 11 是将 CE 设备带进市场的企业。将 CE 设备 9 带进市场的活动包括计划、开发和销售 CE 设备 9。

[0154] 管理中心 3 是管理要包括在 CE 设备 9 中的设备认证信息的组织。管理中心 3 也管理设备认证信息和用于设备认证信息的加密信息的发布。

[0155] 工厂 5 是根据业务组织 11 请求制造 CE 设备 9 的组织。一些情况下，业务组织 11 拥有工厂 5。其它情况下，工厂 5 做为制造 CE 设备 9 的工厂，由业务组织 11 委托的第三方管理。

[0156] 在工厂 5 内部制造的 CE 设备 9 包括由管理中心 3 发布的设备认证信息。

[0157] 设备认证服务器 8 是用地从管理吆 3 接收设备认证证信息及从 CE 设备 9 接收设备认证信息并认证 CE 设备 9 的服务器。

[0158] 设备认证服务器 8 认证的 CE 设备 9 被允许接收一般由服务服务器提供的服务。

[0159] 下面将参照图中所示的标号，解释制造制造 / 认证系统 1 中 CE 设备 9 的处理。(1)：首先，业务组织 11 根据计划设计 CE 设备 9。随后，业务组织 11 从管理中心 3 获取用于创建要安装在 CE 设备 9 中固件的信息。

[0160] 此固件包括一个用于将设备认证信息包括在 CE 设备 9 中的程序和一个用于驱动 CE 设备 9 的程序。固件在工厂 5 时安装在 CE 设备 9 中。业务组织 11 也从管理中心 3 获得用于将设备认证信息包括在 CE 设备 9 中的信息。

[0161] (2)：业务组织 11 请求工厂 5 制造 CE 设备 9，并通过将固件记录到 CD-ROM（光盘 - 只读存储器）或经网络将固件传送到工厂 5，将要安装在 CE 设备 9 中的固件提供到工厂 5。

[0162] (3)：在工厂 5 中，CE 设备 9 组装后，从业务组织 11 收到的固件被安装到 CE 设备 9 中。随后，图 1 所示的连接装置 10 链接到 CE 设备 9 的连接器。因此，工厂 5 请求管理中心 3 将设备认证信息传送到工厂 5。

[0163] (4)：工厂发出请求时，管理中心 3 经网络将要安装在 CE 设备 9 中的设备认证信息传送到工厂 5。传送的设备认证信息是加密信息。

[0164] 由于原始设备认证信息可通过将加密设备认证信息解密而得到，因此，加密的设备认证信息可视为生成原始设备认证信息的源。设备认证信息的内容将在下面详细描述。

[0165] (5)：在工厂 5 中，管理中心 3 传送的设备认证信息经连接装置 10 提供到 CE 设备 9。在通过使用 CE 设备 9 中安装的固件包括的加密密钥将设备认证信息在 CE 设备 9 中解密后，通过使用固件中包括并存储在 CE 设备 9 采用的存储媒体中的另一加密密钥，将解密处理的结果重新加密。

[0166] (6)：随后，根据下面所述的方法，工厂 5 和管理中心 3 验证设备认证信息已正确包括在 CE 设备 9 中。工厂 5 可使用验证结果向管理中心 3 报告制造结果。

[0167] (7)：在工厂 5，在组装 CE 设备 9 的处理和将设备认证信息包括在组装的 CE 设备 9 中的处理完成后，CE 设备 9 可发货。

[0168] (8)：管理中心 3 将 CE 设备 9 的设备认证信息提供到设备认证服务器 8。

[0169] (9)：设备认证服务器 8 请求 CE 设备 9 以将设备认证信息传送到 CE 设备 9，并将从管理中心 3 收到的设备认证信息与从 CE 设备 9 收到的设备认证信息进行比较以便认证 CE 设备 9。

[0170] 图 3 显示了设备认证部分 99 的典型配置。设备认证部分 99 是功能部分，通过在工厂 5 中安装固件而在 CE 设备 9 中形成。

[0171] 设备认证部分 99 包括认证模块 20、写入模块 30、认证信息存储器 40 和主体标识信息存储器 50。

[0172] 认证模块 20 是为设备认证服务器 8 提供用于认证 CE 设备 9 的部件的功能部分。

[0173] 认证模块 20 具有公共密钥 21 和用于生成特有密钥 23 的特有密钥生成器 22。公用密钥 21 和特有密钥 23 在设备认证信息到设备认证服务器 8 的传输中使用。

[0174] 特有密钥 23 是用于将认证信息存储器 40 中存储的设备认证信息加密和解密的密钥。在可以使用特有密钥 23 前，必须从特有密钥生成器 22 和 MAC 地址 51 预先动态生成特有密钥 23。

[0175] MAC 地址 51 是 CE 设备 9 特有的信息。另外，特有密钥 23 也做为 CE 设备 9 特有的密钥生成。

[0176] 在此实施例中，特有密钥 23 通过使用 MAC 地址 51 生成。实际上，特有密钥 23 便可通过使用任何其它信息生成，只要上述其它信息对 CE 设备 9 是特有的信息。上述其它信息的一个示例 i.Link(IEEE 1394) 的地址。

[0177] 也就是说，特有密钥 23 是通过使用对 CE 设备 9 特有的信息，做为也对 CE 设备 9 特有的密钥生成。

[0178] 如上所述，即使在制造的 CE 设备 9 中包括的特有密钥 22 生成器是通用信息，生成的特有密钥 23 也因 CE 设备 9 的不同而异。因此，可轻松管理特有密钥生成器 22。

[0179] 具有上述配置的认证模块 20 从认证信息存储器 40 读出设备认证信息，并在设备认证信息与设备 ID 41 一起传输到设备认证服务器 8 前将其解密。

[0180] 使用后，特有密钥 23 在预定的周期内立即删除。预定的周期可有不同的长度。例如，预定的周期是将设备认证信息加密的处理开始与设备认证部分 99 执行的认证 CE 设备 9 处理结束之间的时期。

[0181] 如上所述，此实施例具有一种配置，其中，特有密钥 23 在使用后被删除。然而，要注意的是，并不是始终必需删除特有密钥 23。

[0182] 写入模块 30 是用于在工厂 5 中将设备认证信息写入 CE 设备 9 的功能部分。

[0183] 写入模块 30 具有预写入密钥 31、特有密钥生成器 32、设备端验证散列函数 34 及服务器端验证散列函数 35。

[0184] 预写入密钥 31 是用于将从管理中心 3 收到的加密设备认证信息解密的密钥。

[0185] 特有密钥生成器 32 是用于生成特有密钥 33 的种子（原始）信息。特有密钥生成器 32 与认证模块 20 的特有密钥生成器 22 相同。

[0186] 特有密钥 33 是用于将由于使用预写入密钥 31 执行的解密处理而获得的设备认证信息加密的密钥。使用特有密钥 33 前，必须通过使用特有密钥生成器 32 和 MAC 地址 51 预先动态生成特有密钥 33。特有密钥 33 与特有密钥 23 相同，在认证模块 20 中生成。

[0187] 具有上述配置的写入模块 30 将从管理中心 3 收到的加密设备认证信息解密，使用特有密钥 33 将解密结果重新加密，并在认证信息存储器 40 中存储重新加密的设备认证信息。

[0188] 在此实施例中，通过在认证信息存储器 40 中存储使用特有密钥 33 加密状态的设备认证信息，可提高设备认证信息的安全。

[0189] 要注意的是也可以提供一种配置，其中，设备认证信息存储在存储单元中而未使

用特有密钥 33 将设备认证信息加密。这种情况下，由于认证模块 20 不需要在认证处理中将设备认证信息解密，因此，不必生成特有密钥 23。

[0190] 设备端验证散列函数 34 是由写入模块 30 用于验证设备认证信息已正确存储在认证信息存储器 40 中的函数。如下面将描述的一样，通过比较从管理中心 3 传送的散列值与使用设备端验证散列函数 34 生成的、作为设备认证信息散列值的散列值，写入模块 30 验证设备认证信息已包括在 CE 设备 9 中。

[0191] 服务器端验证散列函数 35 是用于一个用于生成值的函数，该值由管理中心 3 用于验证设备认证信息已正确存储在认证信息存储器 40 中。

[0192] 如下面将描述的一样，写入模块 30 传送一个散列值到管理中心 3，该值由服务器端验证散列函数 35 生成为存储在认证信息存储器 40 中的设备认证信息散列值。

[0193] 管理中心 3 将从写入模块 30 收到的散列值 30 与通过使用服务器端验证散列值函数生成的、作为发布的设备认证信息散列值的散列值进行比较，以验证设备认证信息已包括在 CE 设备 9 中。

[0194] 从上述说明中看以，实施例提供两种类型的散列函数，即，用于生成在 CE 设备 9 中验证用途的散列值的设备端验证散列函数 34 和用于生成管理服务器 7 中验证用途的散列值的服务器端验证散列函数 35。

[0195] 例如，我们假定相同的散列函数用于 CE 设备 9 和管理服务器 7 中的验证。我们也假定第三方将管理服务器 7 传送到 CE 设备 9 的散列值原样返回到管理服务器 7。这种情况下，管理服务器 7 将难以确定接收的散列值是 CE 设备 9 还是第三方传送的散列值。

[0196] 鉴于上述原因，使用了两种类型的散列函数以防止第三方假装为 CE 设备 9。

[0197] 附带提到的是，散列函数是用于散列电子文本的函数。通过散列电子文本，可从文本中生成对文本特有的字符串。生成的字符串称为电子文本的散列值或文本的摘要消息。

[0198] 从相同的电子文本中获得相同的散列值。即使只修改了部分电子文本，从修改的电子文本获得的散列值也将不同于原始电子文本的散列值。

[0199] 另外，通过对文本的散列值执行逆转换处理，极难获得原始电子文本。

[0200] 如上所述，散列函数是称为单向函数的函数类型，允许轻松地在正向上执行转换处理，但极难执行散列函数的逆转换处理而从由于正向上执行的转换处理所获得的散列值中获得原始值。

[0201] 如上所述，验证秘密信息的一端和保留要验证的秘密信息的一端均生成信息的散列值，并将生成的散列值与从另一端收到的散列值进行比较。这样，两端均能够验证两份秘密信息彼此相同，秘密信息原样保持为机密状态。

[0202] 认证信息存储器 40 是存储用于认证 CE 设备 9 的信息的存储单元。存储的信息包括上述设备认证信息。

[0203] 在该实施例的情况下，存储信息包括上述设备 ID 41 和具有设备 ID 与密码短语 (pass phase) 的加密代码 42。

[0204] 设备 ID 41 是用于标识 CE 设备 9 的 ID 信息。工厂 5 从设备 ID 管理组织预先获得设备 ID 41 并将设备 ID 41 存储在 CE 设备 9 中。

[0205] 具有设备 ID 和密码短语的（设备 ID+ 密码短语）42 包括设备 ID 41 和在设备 ID 41 尾部的加密密码短语。在设备 ID 41 尾部的密码短语已通过使用特有密钥 23 或特有密

钥 33 加密。要注意的是，设备 ID 41 与密码短语的排列顺序可能相反。

[0206] 在下面的说明中，符号（信息 A+ 信息 B）表示由信息 A 和置于信息 A 尾部的信息 B 组成的信息。由于加密（信息 A+ 信息 B）的处理获得的信息称为加密的（信息 A+ 信息 B）。

[0207] 例如，我们假定设备 ID 41 为“123”，并且密码短语为“abc”。这种情况下，具有设备 ID 41 和密码短语的（设备 ID+ 密码短语）42 为 123abc。通过使用特有密钥 23 或特有密钥 33 加密（设备 ID+ 密码短语）处理的结果称为加密的（设备 ID+ 密码短语）42。

[0208] 密码短语是秘密信息，由管理服务器 7 发布，以便在工厂 5 将设备认证信息包括在 CE 设备 9 的处理中包括在设备认证信息中。

[0209] 在此实施例中，（设备 ID+ 密码短语）用做设备认证信息。

[0210] 通过如上所述组合密码短语与设备 ID，可增加设备认证信息量。这样，第三方难以将加密的（设备 ID+ 密码短语）42 解密。因此，可提高设备认证信息的安全。

[0211] 另外，通过比较解密的（设备 ID+ 密码短语）与 CE 设备中接收的设备 ID，也可验证设备 ID 与加密的（设备 ID+ 密码短语）组合是否正确。

[0212] 主体标识信息存储器 50 是存储用于标识 CE 设备 9 主体的信息的存储单元。

[0213] 用于标识 CE 设备 9 主体的信息示例有 MAC（媒体接入控制）地址 51 和称为 i.Link 的信息。在网络中用于标识 CE 设备 9 时，MAC 地址 51 是对 CE 设备 9 特有的信息。

[0214] 具体而言，MAC 地址 51 是 CE 设备 9 唯一的硬件地址。因此，例如即使 CE 设备 9 从一个位置移到网络中的另一位置，MAC 地址 51 也保持不变。

[0215] 随后，下面的说明解释将设备认证信息包括在具有上述配置的 CE 设备 9 中的过程、验证包括的设备认证信息的过程及通过使用包括的设备认证信息认证 CE 设备 9 的过程。

[0216] 图 4 显示了将设备认证信息包括在 CE 设备 9 的准备阶段执行的工作过程的解释中参照的流程图。

[0217] 首先，在第一步骤 10 中，业务组织 11 制定 CE 设备 9 的生产计划。此生产计划工作例如由负责生产计划的个人手动完成。

[0218] 随后，在下一步骤 12 中，业务组织 11 中设定的业务组织系统接入管理服务器 7，以请求用于将设备认证信息包括在 CE 设备 9 采用的写入模块 30 中的预写入密钥 31。

[0219] 管理服务器 7 具有象如图 8 所示表格的密钥表 700。从密钥表 700 中，管理服务器 7 发布预写入密钥 31 和密钥标识符以便在其它预写入密钥中唯一地标识预写入密钥 31。随后，在步骤 20 中，管理服务器 7 将发布的预写入密钥 31 和发布的密钥标识符传送到业务组织系统。

[0220] 业务组织 11 可具有一种配置，请求管理服务器 7 将用于标识产品类型的产品代码和下面要描述的特有密钥生成器传送到业务组织 11。

[0221] 管理服务器 7 管理将产品代码和特有密钥生成器成对管理，每个对由一个产品代码和对应于该产品代码的特有密钥生成器组成。

[0222] 在步骤 14 中，业务组织系统创建用于从管理服务器 7 接收预写入密钥 31 和密钥标识符、并在写入模块 30 中存储预写入密钥 31 的固件。另外，业务组织系统在固件中包括该特有密钥生成器。

[0223] 随后，在下一步骤 16 中，业务组织系统将创建的固件、密钥标识符和用于标识 CE 设备 9 类型的产品代码传送到工厂 5 中设定的工厂系统。

[0224] 在工厂 5 中，产生产品代码标识的多个 CE 设备 9。然而，要注意的是，所有产生的 CE 设备使用相同的预写入密钥 31。为此，创建的固件和密钥标识符可传送到成对工厂，以从形成成对的固件和密钥标识符产生多个 CE 设备 9。

[0225] 工厂系统从业务组织系统接收这些信息。随后，工厂 5 开始制造接收的产品代码标识的 CE 设备 9。

[0226] 在步骤 30 中，工厂系统发布以此方式制造的 CE 设备 9 的产品序列号，即包括固件前制造的产品的产品序列号。

[0227] 指定给 CE 设备 9 的产品序列号是对 CE 设备 9 特有的编号。例如，产品序列号是打印在标签印记上的号码或条形码，而标签印记贴在 CE 设备 9 上以便从 CE 设备 9 外部的位置可查看产品序列号。

[0228] 在此实施例的情况下，指定给 CE 设备 9 的产品序列号是用于标识 CE 设备 9 的信息。然而，要注意的是，例如，产品代码或产品序列号也可用于标识 CE 设备 9。

[0229] 这种情况下，设备认证服务器 8 将产品代码和产品序列号贴到 CE 设备 9 上。

[0230] 也就是说，任何信息只要可用于标识 CE 设备 9 便适用。

[0231] 随后，在下一步骤 32 中，工厂系统将固件包括在 CE 设备 9 中。

[0232] 通过经 CE 设备 9 的连接器将固件提供到 CE 设备 9，固件可包括在 CE 设备 9 中。

[0233] 业务组织 11 可通过将固件存储在诸如 CD-ROM 等记录媒体中，将固件输送到工厂 5。随后，在工厂 5 中，从记录媒体读出要包括在 CE 设备 9 中的固件。

[0234] 通过将固件包括在 CE 设备 9 中，在 CE 设备 9 内创建了图 3 所示的设备认证部分 99。

[0235] 要注意的是，在将固件包括在 CE 设备 9 的处理中，工厂系统将预先从设备 ID 管理机构获得的设备 ID 41 存储在认证信息存储器 40 中。然而，在此阶段，（设备 ID+ 密码短语）42 尚未存储在认证信息存储器 40 中。

[0236] 图 5 显示的流程图表示将设备认证信息包括到 CE 设备 9 中的过程，也就是说，在认证信息存储器 40 中存储（设备 ID+ 密码短语）42 的过程。

[0237] 要注意的是，如下所述将设备认证信息包括到 CE 设备 9 中的处理是用连接到 CE 设备 9 的连接装置 10 执行。

[0238] 工厂系统具有类似于图 8 所示表的密钥标识符管理表 500。密钥标识符管理表 500 是通过将产品代码与其相应密钥标识符相关联、使用从业务组织系统获得的密钥标识符、管理表示产品的产品代码的表。

[0239] 在步骤 40 中，工厂系统接入管理服务器 7 以便请求发布密码短语。另外，工厂系统将以前获得的设备 ID 41 和在密钥标识符管理表 500 中做为 CE 设备 9 的密钥标识符存储的密钥标识符传送到管理服务器 7。

[0240] 在步骤 50 中，管理服务器 7 在收到工厂系统请求发放密码短语的请求时发布密码短语。

[0241] 要注意的是，密码短语是做为字符串创建的秘密信息，包括字符、数字和 / 或符号。密码短语是与密码相同类型的信息。

[0242] 用做秘密信息的相对短的字符串称为密码。另一方面，用做秘密信息的相对长的字符串称为密码短语。对第三方而言，加密的字符串越长，字符串解密就越难。

[0243] 随后，管理服务器 7 从图 8 所示的密钥表获得与已从工厂系统收到的密钥标识符相关联的预写入密钥 31。

[0244] 随后，在下一步骤 52 中，管理服务器 7 从由工厂系统收到的设备 ID 41 和在步骤 50 生成的密码短语生成（设备 ID+ 密码短语），通过使用以前获得的预写入密钥 31 将（设备 ID+ 密码短语）加密以产生加密的（设备 ID+ 密码短语）42。

[0245] 加密的（设备 ID+ 密码短语）用做设备认证信息。

[0246] 管理服务器 7 很类似于 CE 设备 9，具有设备端验证散列函数 34 和服务器端验证散列函数 35。随后，在下一步骤 54 中，设备端验证散列函数 34 用于生成以前生成的（设备 ID+ 密码短语）的散列值。（设备 ID+ 密码短语）的散列值称为第一散列值。

[0247] 第一散列值在 CE 设备 9 中用于确定设备认证信息是否已正确包括。

[0248] 要注意的是，服务器端验证散列函数 35 生成要在管理服务器 7 中用于确定设备认证信息是否已正确包括在管理服务器 7 中的散列值。

[0249] 随后，在下一步骤 56 中，管理服务器 7 传送设备 ID 41、上述生成的加密的（设备 ID+ 密码短语）42 及第一散列值到工厂系统。这种情况下，管理服务器 7 充当源信息提供装置。

[0250] 要注意的是，管理服务器 7 也具有图 8 所示发布的设备认证信息表 702。在管理服务器 7 将设备 ID 41、加密的（设备 ID+ 密码短语）42 和第一散列值传送到工厂系统时，管理服务器 7 也更新发布的设备认证信息表 702。

[0251] 因此，发布的密码短语可与设备 ID 41 和密钥标识符相关联。

[0252] 在步骤 42，工厂系统从管理服务器 7 接收这些信息，并将它们经连接装置 10 提供给 CE 设备 9。

[0253] 在步骤 60，在 CE 设备 9 中采用的写入模块 30 接收这些信息。加密的（设备 ID+ 密码短语）42 与源信息对应。因此，这种情况下，写入模块 30 充当源信息获取装置。

[0254] 第一散列值与通过使用单向功能对设备认证信息执行的转换处理的结果对应。因此，写入模块 30 具有转换值获取装置。

[0255] 随后，在下一步骤 62 中，写入模块 30 通过使用预写入密钥 31 将加密的（设备 ID+ 密码短语）42 解密。

[0256] 通过执行解密处理，CE 设备 9 能够获得从管理中心 3 收到的设备认证信息。这种情况下，设备认证信息是（设备 ID+ 密码短语）。

[0257] 如上所述，写入模块 30 具有生成装置，用于从源信息生成设备认证信息。

[0258] CE 设备 9 可将解密的（设备 ID+ 密码短语）原样保存在存储器中。然而，在此实施例的情况下，（设备 ID+ 密码短语）在存储在存储器中之前被重新加密，以便增强设备认证信息的安全。

[0259] 为执行重新加密处理，首先，写入模块 30 在下一步骤 64 中从 MAC 地址 51 和特有密钥生成器 32 生成特有密钥 33。

[0260] 此步骤执行的目的是获得对 CE 设备 9 特有的加密密钥。例如，此步骤执行的目的是通过使用 MAC 地址 51 获得特有密钥 33。然而，此步骤的目的不限于此示例。通过使用对

CE 设备 9 而言特有的任何信息，也可执行该步骤。例如，可使用产品序列号。

[0261] 另外，如下面将描述的一样，认证模块 20 也能够生成与特有密钥 33 相同的加密密钥。因此，写入模块 30 和认证模块 20 均具有密钥生成装置。

[0262] 随后，在下一步骤 66 中，写入模块 30 通过使用生成的特有密钥 33，将（设备 ID+ 密码短语）加密以生成加密的（设备 ID+ 密码短语）42。

[0263] 要注意的是，由于在重新加密处理中使用的加密密钥不同于加密处理中使用的加密密钥，因此，加密的（设备 ID+ 密码短语）42 不同于从管理服务器 7 收到的加密的（设备 ID+ 密码短语）。

[0264] 随后，在下一步骤 68 中，写入模块 30 将加密的（设备 ID+ 密码短语）42 提供到认证信息存储器 40。随后，在步骤 70 中，认证信息存储器 40 在其中存储加密的（设备 ID+ 密码短语）42。

[0265] 要注意的是，在设备认证部分 99 假定为删除特有密钥 33 的配置情况下，特有密钥 33 在使用后由密钥删除装置立即删除。

[0266] 如上所述，加密的（设备 ID+ 密码短语）42 对 CE 设备 9 和使用动态生成的特有密钥 33 进行的加密处理的结果而言是特有的。因此，可提高加密的（设备 ID+ 密码短语）42 的安全。

[0267] 认证信息存储器 40 充当存储装置。

[0268] 根据上述过程，管理服务器 7 发布的设备认证信息可包括在 CE 设备 9 中。

[0269] 另外，由于设备认证信息以其加密状态原样提供到 CE 设备 9，因此，可在工厂 5 预先防止设备认证信息泄漏。因此，可在设备认证信息包括在 CE 设备 9 中时提高所需的安全。

[0270] 最重要的是，由于设备认证信息通过使用对 CE 设备 9 特有的加密密钥，以重新加密状态存储在 CE 设备 9 中，因此，可在 CE 设备 9 发货后预先防止设备认证信息从 CE 设备 9 泄漏。因此，可提高 CE 设备 9 发货后所需的安全。

[0271] 图 6 显示了由管理中心 3 和工厂 5 执行的过程解释中参照的流程图，该过程是用于验证设备认证信息已正确包括到 CE 设备 9 中的过程。

[0272] 此过程通过已经连接到 CE 设备 9 的连接装置 10 执行。通常，该过程在工厂系统将设备认证信息包括到 CE 设备 9 后自动执行。

[0273] 首先，在步骤 90 中，设备认证部分 99 中采用的写入模块 30 从认证信息存储器 40 读出加密的（设备 ID+ 密码短语）42。在此步骤中，加密的（设备 ID+ 密码短语）从认证信息存储器 40 传到写入模块 30。

[0274] 随后，在步骤 100 中，写入模块 30 从特有密钥生成器 32 和 MAC 地址 51 生成特有密钥 33。随后，在下一步骤 102 中，写入模块 30 通过使用特有密钥 33 将加密的（设备 ID+ 密码短语）42 解密。

[0275] 随后，在下一步骤 104 中，写入模块 30 通过使用设备端验证散列函数 34，生成解密的（设备 ID+ 密码短语）的散列值。解密的（设备 ID+ 密码短语）散列值称为第一散列值。

[0276] 随后，在下一步骤 106 中，写入模块 30 将从管理服务器 7 收到第一散列值与在步骤 104 中生成的散列值进行比较，以产生两个散列值是否彼此相等的确定结果。

[0277] 因此，写入模块 30 具有用于计算第一散列值的转换值计算装置和确定装置。

[0278] 表示两个散列值彼此相等的确定结果也证明管理服务器 7 生成的（设备 ID+ 密码短语）与认证信息存储器 40 中存储的（设备 ID+ 密码短语）相匹配。

[0279] 随后，在下一步骤 108 中，写入模块 30 通过使用服务器端验证散列函数 35 生成（设备 ID+ 密码短语）的散列值。通过使用服务器端验证散列函数 35 生成的（设备 ID+ 密码短语）的散列值称为第二散列值。

[0280] 随后，在下一步骤 110 中，写入模块 30 从认证信息存储器 40 读出设备 ID 41，将在步骤 106 中获得的确定结果做为第一散列值、设备 ID 41 和第二散列值的比较结果，传送到工厂系统。第二散列值也传送到管理服务器 7。

[0281] 从上述说明中可看到，写入模块 30 具有转换值计算装置和转换值提供装置。

[0282] 基于从 CE 设备 9 收到的比较结果，工厂能够知道设备认证信息是否已正确包括在 CE 设备 9 中。

[0283] 另一方面，如果第一散列值彼此不等，则设备 ID 41 被丢弃，并且通过使用新设备 ID 再次尝试将设备认证信息包括在 CE 设备 9 中。

[0284] 导致信息包括失败的设备 ID 41 也可重新利用。然而，在该实施例的情况下，导致信息包括失败的设备 ID 41 被丢弃以防止在市场上错误销售具有同一设备 ID 的多个 CE 设备 9。

[0285] 要注意的是，在常规制造处理中，为保持设备认证信息的机密，在设备认证信息一旦已包括在 CE 设备 9 中后，难以确定设备认证信息是否已正确包括在 CE 设备 9 中，并且在一些情况下，设备认证信息已正确包括在 CE 设备 9 中的事实不验证。

[0286] 然而，在此实施例的情况下，设备认证信息的散列值在 CE 设备 9 中互相比较。因此，可确定 CE 设备 9 内设备认证信息是否已正确包括在 CE 设备 9 中，将设备认证信原样机密保持。

[0287] 验证设备认证信息忆正确包括在 CE 设备 9 中后，在步骤 120 中，工厂系统将设备 ID 41 和第二散列值（已从 CE 设备 9 收到），及指定给 CE 设备 9 的产品序列号一起传送到管理服务器 7。

[0288] 在步骤 130 中，管理服务器 7 从工厂系统接收这些信息并搜索图 8 所示的发布的设备认证信息表 702，以查找对应于收到的设备 ID 41 的密码短语。

[0289] 因此，管理服务器 7 具有转换值获取装置，用于获取第二散列值。

[0290] 随后，管理服务器 8 从设备 ID 41 和在搜索操作中找到的密码短语生成（设备 ID+ 密码短语），通过使用服务器端验证散列函数 35 产生（设备 ID+ 密码短语）的第二散列值。因此，管理服务器 7 具有转换值计算装置。

[0291] 随后，在下一步骤 132 中，管理服务器 7 将从工厂系统收到的第二散列值与生成的第二散列值进行比较，以确定两个第二散列值是否彼此相等。因此，管理服务器 7 具有确定装置。

[0292] 如果发现两个第二散列值彼此相等，则管理服务器 7 确定设备认证信息已成功包括在 CE 设备 9 中。

[0293] 另一方面，如果发现两个第二散列值彼此不等，则管理服务器 7 确定设备认证信息未成功包括在 CE 设备 9 中。

[0294] 管理服务器 7 具有象图 8 所示表的设备认证表 704。设备认证表 704 是用于通过

将设备 ID 41、密码短语和产品序列号彼此相关联而存储设备 ID 41、密码短语和产品序列号的表。

[0295] 在步骤 134，如果发现两个第二散列值彼此相等，则管理服务器 7 将设备 ID 41、密码短语和产品序列号存储在设备认证表 704 中。

[0296] 要注意的是，设备认证表 704 提供到设备认证服务器 8，由设备认证服务器 8 在认证 CE 设备 9 中使用。因此，管理服务器 7 在此情况下充当设备认证信息提供装置。

[0297] 随后，在步骤 136 中，管理服务器 7 将从工厂系统收到数据的日期添加到数据。从工厂系统收到的数据是设备 ID 41、产品序列号和第二散列值。随后，管理服务器 7 在将带有日期的数据传送到工厂前，将数字签名做为秘密密钥添加到带日期的数据上。这种情况下，管理服务器 7 充当确定结果传输装置。

[0298] 在步骤 122 中，充当源信息包括主组织的工厂系统从管理服务器 7 接收带日期的数据，并确认设备认证信息已正确包括在 CE 设备 9 中。

[0299] 这样，工厂系统能够确认设备 ID 41、产品序列号和第二散列值已由管理服务器 7 接收。设备 ID 41、产品序列号和第二散列值可视为制造结果。

[0300] 随后，工厂 5 将完成制造处理的 CE 设备 9 发货。

[0301] 图 7 显示了设备认证服务器 8 采用的过程解释中参照的流程图，该过程用于认证 CE 设备 9。

[0302] 首先，在步骤 140 中，如图 3 所示设备认证部分 99 中采用的认证模块 20 从认证信息存储器 40 读出加密的（设备 ID+ 密码短语）42。因此，（设备 ID+ 密码短语）42 从认证信息存储器 40 传到认证模块 20。

[0303] 随后，在步骤 150 中，认证模块 20 通过使用特有密钥生成器 22 和 MAC 地址 51 生成特有密钥 23。

[0304] 随后，在下一步骤 152 中，认证模块 20 通过使用特有密钥 23 将加密的（设备 ID+ 密码短语）42 解密，以获得（设备 ID+ 密码短语），并在下一步骤 154 中将（设备 ID+ 密码短语）传送到设备认证服务器 8。因此，认证模块 20 具有设备认证信息传输装置。

[0305] 要注意的是，在 CE 设备 9 与设备认证服务器 8 之间的通信路径是通过使用诸如 SSL（安全套接层）等加密技术确保交换数据安全的路径。

[0306] 在步骤 160 中，设备认证服务器 8 从 CE 设备 9 接收（设备 ID+ 密码短语），并通过使用对应于公共密钥 21 的秘密密钥将（设备 ID+ 密码短语）解密。随后，设备认证服务器 8 将解密的密码短语与存储在从管理中心 3 收到的设备认证表 704 中的密码短语进行比较，以认证 CE 设备 9。

[0307] 随后，在下一步骤 162 中，设备认证服务器 8 从设备认证表 704 标识 CE 设备 9 的产品序列号。

[0308] 此步骤是认证 CE 设备的过程结尾。

[0309] 图 9 显示了 CE 设备 9 的典型硬件配置。

[0310] CPU（中央处理器）121 是通过执行事先存储在 ROM（只读存储器）122 中的程序或从存储部分 128 载入 RAM（随机存取存储器）123 中的程序，用于执行各种处理的中央处理部分。

[0311] ROM 122 是用于存储执行 CE 设备 9 的功能所必需的基本程序和存储诸如参数等数

据的存储器。

[0312] RAM 123 是做为 CPU 121 执行各种处理所需工作区域的存储器。

[0313] 存储部分 128 是用于存储执行 CE 设备 9 功能所必需的其它程序和存储数据的单元。存储部分 128 的示例有硬盘和半导体存储器。

[0314] 在业务组织 11 中创建的固件在工厂 5 中存储在存储部分 128。CPU 121 执行固件以生成图 3 所示、做为设备认证部分 99 要素的各种配置要素。

[0315] 存储部分 128 中存储的其它程序包括用于输入和输出文件、控制 CE 设备 9 组件和执行基本功能的 OS(操作系统)。

[0316] CPU 121、ROM 122 和 RAM 123 通过总线 124 彼此连接。此总线 124 也连接到输入/输出接口 125。

[0317] 输入/输出接口 125 连接到输入部分 126、输出部分 127、上述存储部分 128 及通信部分 129。输入部分 126 包括键盘和鼠标,而输出部分 127 包括显示单元和扬声器。显示单元可以是 CRT(阴极射线管)显示单元或 LCD(液晶显示)单元。存储部分 128 一般包括硬盘。通信部分 129 具有调制解调器或终端适配器。

[0318] 通信部分 129 是用于执行通过网络与其它设备进行的通信处理的功能单元。例如,通信部分 129 连接到连接装置 10 以接收设备认证信息,或连接到设备认证服务器 8 以执行认证 CE 设备 9 处理的通信。

[0319] 如有必要,输入/输出接口 125 也连接到正确安装有记录媒体的驱动器 140。记录媒体可以是磁盘 141、光盘 142、磁光盘 143 或存储卡 144。如上所述,如有必要,CPU 121 要执行的计算机程序从存储部分 128 载入 RAM 123。

[0320] 要注意的是,由于管理服务器 7 和设备认证服务器 8 的配置基本上与 CE 设备 9 的配置相同,因此,不提供管理服务器 7 和设备认证服务器 8 的配置解释。

[0321] 根据上述第一实施例,认证 CE 设备 9 的处理中做为设备认证信息所需的(设备 ID+ 密码短语)可从管理服务器 7 传送到具高安全性的 CE 设备 9。另外,工厂 5 和管理服务器 7 能够验证设备认证信息已正确包括在 CE 设备 9 中。

[0322] 下面通过比较该实施例与常规系统,解释了上述第一实施例提供的效果。

[0323] (1):在常规系统中,由于用做设备认证信息的(设备 ID+ 密码短语)是提供到 CE 设备 9 的明文,因此,工厂 5 的工人或其它人士很可能意外或有意看到设备认证信息。另一方面,在此实施例的情况下,通过以加密状态原样将(设备 ID+ 密码短语)提供到 CE 设备 9,可解决该问题。

[0324] (2):在常规系统中,例如,即使设备认证信息在传送到工厂 5 前已加密,将设备认证信息包括到 CE 设备 9 中的方法因产品不同和工厂不同而异,使得难以提供统一的技术。因此,很可能导致安全级别分散。另一方面,在此实施例的情况下,采用将设备认证信息包括在 CE 设备 9 的共用方法以减少安全级别的分散量。

[0325] (3):在常规系统系统情况下,加密密钥可能被泄漏并影响另一 CE 设备 9。另一方面,在此实施例情况下,为每个 CE 设备 9 生成特有密钥 23,做为对生成特有密钥 23 的 CE 设备 9 特有的密钥。因此,即使特有密钥 23 泄漏出,特有密钥 23 也不影响另一 CE 设备 9。

[0326] 关于预写入密钥 31,可通过为每个产品或每个周期生成预写入密钥 31 而限制影响范围。

[0327] (4)：在常规系统的情况下，在工厂 5 或充当发布设备认证信息的发起者的管理中心 3 中，难以验证设备认证信息已正确包括到 CE 设备 9 中。另一方面，在此实施例的情况下，通过使用诸如散列值等特有信息，可在工厂 5 或管理中心 3 中验证设备认证信息已正确包括在 CE 设备 9 中。

[0328] (5)：在常规系统的情况下，工厂 5 难以验证管理中心 3 正确收到了有关制造结果的报告。另一方面，在此实施例的情况下，管理服务器 7 将日期添加到从工厂系统收到数据，并在将带日期的数据传送到工厂系统前在带日期数据上添加数字签名。

[0329] (6)：在常规系统的情况下，难以使用诸如电子证书等其它信息做为设备认证信息。另一方面，在此实施例的情况下，本发明可使用电子证书应用到认证方法。

[0330] 在该实施例的情况下，例如，设备认证信息经网络传送到工厂 5，并通过连接装置 10 提供到 CE 设备 9。然而，要注意的是，由于设备认证信息以加密状态提供到 CE 设备 9，因此，也可提供一种配置，其中，设备认证信息记录到诸如 CD-ROM 等存储媒体上，并且存储媒体随后送到工厂 5 以便工厂 5 能够将设备认证信息从媒体传到 CE 设备 9。

[0331] 另外，在该实施例的情况下，例如，提供了一种配置，其中，通过使用预写入密钥 31，将从管理服务器 7 收到的加密的（设备 ID+ 密码短语）解密，然后存储在认证信息存储器 40 中。然而，也可提供另一种配置，其中，从管理服务器 7 收到的加密的（设备 ID+ 密码短语）立即存储在认证信息存储器 40 中而不解密，并只在认证处理中使用前通过使用预写入密钥将其解密。

[0332] 下面，将解释第二实施例。

[0333] [第二实施例概述]

[0334] 图 10 是简单显示第二实施例的示范图

[0335] 在该实施例的情况下，在生成设备认证信息的处理中，通过使用管理服务器 7 和 CE 设备 9 中相同的逻辑，充当生成设备认证信息的源信息被转换成设备认证信息。例如，源信息被加密，以便在管理服务器 7 和 CE 设备 9 中使用同一加密密钥的同一加密处理中生成设备认证信息。

[0336] 首先，管理服务器 7 将源信息传送到工厂 5，并在生成设备认证信息的处理中将源信息转换成设备认证信息。

[0337] 另一方面，在工厂 5 中，源信息经连接装置 10 提供到 CE 设备 9。随后，CE 设备 9 将收到的源信息转换成设备认证信息。

[0338] 从上述说明中可以看到，管理服务器 7 和 CE 设备 9 因此能够共享相同的设备认证信息。

[0339] 另外，即使源信息泄漏给他人，除非他知道将源信息转换成设备认证信息的逻辑，否则，该人也将无法知道设备认证信息。

[0340] 如上所述，由于设备认证信息通过 CE 设备 9 中的内部部分生成，因此，可防止设备认证信息在工厂 5 以明文形式输出。

[0341] [第二实施例详情]

[0342] 制造 / 认证系统 1 的配置是图 2 所示配置，与根据第一实施例的配置相同，并且设备认证部分 99 的配置是图 3 所示配置，与根据第一实施例的配置相同。因此，将不重复这些配置的解释。

[0343] 另外，第二实施例中采用的每个配置要素，做为与第一实施例中采用的其对应物相同的配置，通过将该配置要素表示为与对应物相同的标号进行解释。

[0344] 在下面的说明中，通过参照流程图解释将设备认证信息包括到 CE 设备 9 中、验证所述包括并认证 CE 设备 9 的方法。

[0345] 要注意的是，由于设备认证信息到 CE 设备 9 中的包括的准备与第一实施例中的相同，因此，将不重复参照图 4 的解释。

[0346] 管理服务器 7 很类似于第一实施例，具有象图 14 所示表的密钥表 706。密钥表 706 是用于通过将密钥标识符与预写入密钥 31 彼此相关而管理密钥标识符和预写入密钥 31 的表。

[0347] 图 11 显示了将设备认证信息包括到 CE 设备 9 的过程解释中参照的流程图。

[0348] 在该过程，CE 设备 9 已经组装，并且连接装置 10 已链接到连接装置 10 的连接器。

[0349] 首先，在步骤 200 中，工厂系统请求管理服务器 7 发布密码短语，并将预先从设备 ID 管理组织获得的设备 ID 41 传送到管理服务器 7。

[0350] 要注意的是，设备 ID 41 也存储在认证信息存储器 40 中。

[0351] 在步骤 210 中，管理服务器 7 发布密码短语以响应工厂系统做出的请求。

[0352] 管理服务器 7 也具有类似于图 14 所示表的发布的设备认证信息表 708。发布的设备认证信息表 708 是用于通过将从工厂系统收到的设备 ID 41 与为设备 ID 41 发布的密码短语彼此相关联，存储设备 ID 41 和密码短语的表。

[0353] 随后，在下一步骤 212 中，在发布密码短语后，管理服务器 7 将密码短语与收到的设备 ID 41 相关联，将密码短语和收到的设备 ID 41 存储在发布的设备认证信息表 708 中。

[0354] 随后，在下一步骤 214 中，管理服务器 7 从设备 ID 41 和发布的密码短语生成（设备 ID+ 密码短语），并将（设备 ID+ 密码短语）传送到工厂系统。

[0355] （设备 ID+ 密码短语）将变为用于生成设备认证信息的源信息。

[0356] 在步骤 202 中，工厂系统从管理服务器 7 接收（设备 ID+ 密码短语）。随后，在下一步骤 204 中，工厂系统经连接装置 10 将（设备 ID+ 密码短语）提供到 CE 设备 9。

[0357] 在步骤 220 中，CE 设备 9 中采用的写入模块 30 接收（设备 ID+ 密码短语）。随后，在下一步骤 222 中，写入模块 30 通过使用预写入密钥 31 将（设备 ID+ 密码短语）加密以生成加密物（设备 ID+ 密码短语）42。

[0358] 在此实施例的情况下，（设备 ID+ 密码短语）用做加密处理中用于生成（设备 ID+ 密码短语）42 的源信息，而该（设备 ID+ 密码短语）42 用做设备认证信息。

[0359] 也就是说，（设备 ID+ 密码短语）转换成由于转换处理而获得的加密的（设备 ID+ 密码短语）42，该处理采用了使用预写入密钥 31 的转换技术。加密的（设备 ID+ 密码短语）42 随后用做设备认证信息。

[0360] 随后，在下一步骤 224 中，写入模块 30 从特有密钥生成器 32 和 MAC 地址 51 生成特有密钥 33。随后，在下一步骤 226 中，写入模块 30 通过使用生成的特有密钥 33 将加密的（设备 ID+ 密码短语）42 重新加密。

[0361] 这是因为在此实施例的情况下，加密的（设备 ID+ 密码短语）42 本身用做设备认证信息。因此，通过将加密的（设备 ID+ 密码短语）42 以再加密的状态保留在 CE 设备 9 中，可进一步增强设备认证信息的安全。

[0362] 在下面的说明中，以再加密状态保持的加密的（信息 A+ 信息 B）称为重新加密的（信息 A+ 信息 B）。

[0363] 在此特殊情况下，以再加密状态保持的加密的（设备 ID+ 密码短语）42 称为重新加密的（设备 ID+ 密码短语）42a。随后，在下一步骤 228 中，写入模块 30 在认证信息存储器 40 中写入重新加密的（设备 ID+ 密码短语）42a。随后，在下一步骤 230 中，重新加密的（设备 ID+ 密码短语）42a 存储在认证信息存储器 40 中。

[0364] 如上所述，在此实施例的情况下，设备 ID 41 和重新加密的（设备 ID+ 密码短语）42a 存储在认证信息存储器 40 中。

[0365] 图 12 显示了在管理中心 3 和工厂 5 为验证设备认证信息已正确包括在 CE 设备 9 而执行的过程解释中参照的流程图。

[0366] 此过程是通过已经链接到 CE 设备 9 连接器的连接装置 10 执行。通常，该过程在工厂系统将设备认证信息包括在 CE 设备 9 中之后自动执行。

[0367] 首先，在步骤 240 中，写入模块 30 从认证信息存储器 40 中读出重新加密的（设备 ID+ 密码短语）42a。因此，重新加密的（设备 ID+ 密码短语）42a 从认证信息存储器 40 传到写入模块 30。

[0368] 随后，在步骤 250 中，写入模块 30 从特有密钥生成器 32 和 MAC 地址 51 生成特有密钥 33。随后，在下一步骤 252 中，写入模块通过使用特有密钥 33 将重新加密的（设备 ID+ 密码短语）42a 解密以生成加密的（设备 ID+ 密码短语）42。

[0369] 随后，在步骤 254 中，写入模块 30 通过使用服务器端验证散列函数 35 从加密的（设备 ID+ 密码短语）42 生成第二散列值，并在下一步骤 256 中将第二散列值传送到工厂系统。

[0370] 在第一实施例的情况下，第二散列值从（设备 ID+ 密码短语）生成。另一方面，在第二实施例的情况下，第二散列值从加密的（设备 ID+ 密码短语）42 生成。

[0371] 要注意的是，在第二实施例的情况下，不使用第一散列值。

[0372] 在步骤 260 中，工厂系统将设备 ID 41、产品序列号和密钥标识符添加到从 CE 设备 9 接收的第二散列值，将设备 ID 41、产品序列号、密钥标识符和第二散列值传送到管理服务器 7。

[0373] 在步骤 270 中，管理服务器 7 搜索图 14 所示发布的设备认证信息表 708，查找做为发布到 CE 设备 9 的密码短语、对应于从工厂系统收到的设备 ID 41 的一个密码短语。

[0374] 随后，在下一步骤 272 中，管理服务器 7 搜索密钥表 706，查找做为与 CE 设备 9 中存储的相同的预写入密钥 31、对应于从工厂系统收到的密钥标识符的一个预写入密钥 31。

[0375] 随后，在下一步骤 274 中，管理服务器 7 从工厂系统收到的设备 ID 41 和在步骤 270 执行的搜索处理中获得的密码短语生成（设备 ID+ 密码短语），通过使用在步骤 272 执行的搜索处理中获得的预写入密钥 31 将生成的（设备 ID+ 密码短语）加密以生成加密的（设备 ID+ 密码短语）42。

[0376] 随后，在下一步骤 276 中，管理服务器 7 通过使用服务器端验证散列函数 35，从生成的加密的（设备 ID+ 密码短语）42 生成第二散列值。

[0377] 随后，在下一步骤 278 中，管理服务器 7 比较在步骤 276 中生成的第二散列值和从工厂系统收到的第二散列值以验证设备认证信息已正确包括在 CE 设备 9 中。

[0378] 管理服务器 7 具有象 14 所示表的设备认证表 710。设备认证表 710 是用于通过将设备 ID 41、加密的（设备 ID+ 密码短语）42、产品序列号和密钥标识彼此相关联而存储这些要素的表，每个加密的（设备 ID+ 密码短语）42 均用做设备认证信息。

[0379] 随后，在下一步骤 280 中，从第二散列值彼此相比较的结果而知道设备认证信息已正确包括在 CE 设备 9 中，管理服务器 7 依据第二散列值的比较结果，通过将设备 ID 41、加密的（设备 ID+ 密码短语）42、产品序列号和密钥标识彼此相关联而在设备认证表中存储这些要素。

[0380] 要注意的是，设备认证表 710 提供到设备应用服务器 8 以便在认证 CE 设备 9 的处理中使用。

[0381] 随后，在下一步骤 282 中，管理服务器 7 将从工厂系统收到数据的日期添加到数据，并在将带有日期的数据传送到工厂系统前，通过使用秘密密钥将数字签名添加到带日期的数据上。

[0382] 在步骤 262 中，工厂系统验证数字签名以确认设备认证信息已正确包括在 CE 设备 9 中。

[0383] 在验证设备认证信息已包括在 CE 设备 9 中的事实后，CE 设备 9 从工厂 5 发货以进入市场。

[0384] 图 13 显示了设备认证服务器 8 采用的过程解释中参照的流程图，该过程做为认证 CE 设备 9 的过程。

[0385] 首先，在步骤 290 中，如图 3 所示设备认证部分 99 中采用的认证模块 20 从认证信息存储器 40 读出重新加密的（设备 ID+ 密码短语）42a。因此，重新加密的（设备 ID+ 密码短语）42a 从认证信息存储器 40 传到认证模块 20。

[0386] 随后，在步骤 300 中，认证模块 20 通过使用特有密钥生成器 22 和 MAC 地址 51 生成特有密钥 23。

[0387] 随后，在下一步骤 302 中，认证模块 20 通过使用特有密钥 23 将重新加密的（设备 ID+ 密码短语）42a 解密，以生成加密的（设备 ID+ 密码短语）42。随后，在下一步骤 304 中，认证模块通过使用公共密钥 21 将加密的（设备 ID+ 密码短语）42 加密后与设备 ID 41 一起传送到设备认证服务器 8。

[0388] 在步骤 310 中，设备认证服务器 8 从 CE 设备 9 接收加密的（设备 ID+ 密码短语）42，并通过使用对应于公共密钥 21 的秘密密钥，将加密的（设备 ID+ 密码短语）42 解密。随后，设备认证服务器 8 搜索从管理中心 3 收到的设备认证表 710，查找做为 CE 设备 9 的加密的（设备 ID+ 密码短语）42、对应于设备 ID 41 的加密的（设备 ID+ 密码短语）42。设备认证服务器 8 随后比较在搜索处理中找到的加密的（设备 ID+ 密码短语）42 和接收的加密的（设备 ID+ 密码短语）42 以认证 CE 设备 9。

[0389] 随后，在下一步骤 312 中，设备认证服务器 8 搜索设备认证表 710，查表作为 CE 设备 9 的产品序列号、对应于设备 ID 41 的产品序列号。

[0390] 因此，通过执行上述过程，可认证 CE 设备 9。

[0391] 下面通过比较实施例与具有问题的常规系统，解释上述第二实施例提供的效果。

[0392] (1)：在常规系统的情况下，为请求管理服务器 7 传送设备认证信息，必需请求对应于 CE 设备 9 中存储的预写入密钥 31 的加密的密码短语。然而，在此实施例的情况下，可

请求管理服务器 7 传送（设备 ID+ 密码短语）而无需知道 CE 设备 9 中存储的预写入密钥 31。

[0393] (2)：在常规系统的情况下，制造 CE 设备 9 的处理停止时，获取的（设备 ID+ 密码短语）42 变得无用。然而，在此实施例的情况下，从管理服务器 7 获取的（设备 ID+ 密码短语）可由任一 CE 设备利用。因此，如果一个（设备 ID+ 密码短语）被留下，则该（设备 ID+ 密码短语）可提供到另一 CE 设备 9。

[0394] (3)：在常规系统的情况下，如果将 CE 设备 9 的制造线考虑在内，则无法对每个预写入密钥 31 进行自由设定。另一方面，在此实施例的情况下，可设定每个预写入密钥 31 而无需担心制造线。

[0395] 在此实施例的情况下，设备认证信息在管理服务器 7 中从源信息生成，并提供到设备认证服务器 8。这种情况下，源信息是（设备 ID+ 密码短语），并且设备认证信息是加密的（设备 ID+ 密码短语）。然而，要注意的是，本发明的范围并不限于此类配置。例如，可提供一种配置，其中，管理服务器 7 将源信息提供到设备认证服务器 8，而该服务器随后从源信息生成设备认证信息。

[0396] [第三实施例]

[0397] 下面将解释第三实施例。

[0398] 此实施例更新一个应用，该应用包括用于将设备认证信息加密和解密的密钥。在下面的说明中，应用称为设备认证客户机。

[0399] 设备认证客户机安装在CE设备或个人计算机中，形成与图3所示设备认证部分99相同的那些模块。为与公共密钥 21 对应的公共密钥设定使用限制和其它方面。一些情况下，必需将公共密钥更新为新的。

[0400] 在常规系统的情况下，更新公共密钥时，必需将所有设备认证客户机替换为新的。

[0401] 在此实施例的情况下，通过将设备认证客户机中包括的模块替换为一个模块，该模块对应于设备认证部分 99 中包括的一个模块，更新该模块中包括的公共密钥。

[0402] 例如，在更新 CE 设备 9 的设备认证部分 99 的情况下，以下说明例示了由图 15 流程图表示的更新过程。

[0403] 要注意的是，更新服务器是用于提供服务以更新设备认证客户机的服务器。更新服务器和设备认证服务器同步保留各用于标识产品类型的产品代码与特有密钥生成器之间的关系。

[0404] 对象设备是具有要更新的设备认证客户机的终端。

[0405] 首先，在步骤 400 中，对象设备接入更新服务器以便请求模块更新，该模块是包括在设备认证客户机中的设备认证部分 99。

[0406] 在步骤 410 中，更新服务器请求认证对象设备，以响应对象设备所做的请求。

[0407] 在步骤 402 中，对象设备接入设备认证服务器。随后，在步骤 422 中，设备认证服务器认证对象设备。

[0408] 在那时，设备认证服务器发布一次性 ID(one-time ID)，并通过将一次性 ID 与指定给对象设备的产品代码相关联而在存储器中存储一次性 ID。设备认证服务器随后将此一次性 ID 传送到对象设备。

[0409] 在步骤 404 中，对象设备从设备认证服务器接收一次性 ID，并将一次性 ID 传送到

更新服务器。

[0410] 在步骤 412 中，更新服务器从对象设备接收一次性 ID 并将一次性 ID 传送到设备认证服务器。

[0411] 在步骤 424 中，设备认证服务器从更新服务器接收一次性 ID，并将与一次性 ID 相关联的产品代码传送到更新服务器。

[0412] 更新服务器从设备认证服务器接收产品代码，并从产品代码中标识要更新的设备认证客户机。

[0413] 随后，在步骤 406 和 414 中，更新服务与对象设备进行通信，以便通过例如比较对象设备端的设备认证客户机版本与最近的版本，确认要下载的模块。

[0414] 然后在步骤 416，更新服务器搜索对应于产品代码的特定密钥生成器。随后在下一步骤 418，更新服务器生成对应于特定密钥生成器的模块。

[0415] 在那时，模块中包括的公共密钥是最近的密钥。

[0416] 随后，在下一步 420 中，更新服务器将生成的模块下载到对象设备。

[0417] 在步骤 408 中，对象设备保存下载的模块。

[0418] 如上所述，在此实施例的情况下，通过更新模块，可更新模块中包括的公共密钥。

[0419] [第四实施例]

[0420] 在第一实施例的情况下，CE 设备 9 生成第二散列值，将第二散列值传送到管理服务器 7，并且管理服务器 7 验证第二散列值。另一方面，在第四实施例的情况下，CE 设备 9 将验证第一散列值的处理结果传送到管理服务器 7。

[0421] 图 16 显示了设备认证部分 99a 的典型配置。第四实施例中采用的每个配置要素，作为与第一实施例中采用的其对应物相同的配置时，通过将该配置要素表示为与对应物相同的标号进行解释，并且要素的解释将不提供。

[0422] 设备认证部分 99a 具有认证信息写入验证模块 36，用于将验证第一散列值的处理结果传送到管理服务器 7。

[0423] 由于不必将第二散列值传送到管理服务器 7，因此，写入模块 30a 不包括图 3 所示的服务器端验证散列函数 35。

[0424] 写入模块 30a 是用于比较从管理中心 3 收到的第一散列值和通过使用设备端验证散列函数 34 生成的第一散列值的单元，并且它将比较结果输出到认证信息写入验证模块 36。

[0425] 认证信息写入验证模块 36 还获取设备 ID，将设备 ID 和验证结果经连接装置 10 传送到工厂系统。

[0426] 工厂系统将设备 ID 和验证结果与序列号一起传递到管理中心 3 中采用的管理服务器 7。从验证结果中，管理中心 3 能够确认设备认证信息已包括在 CE 设备 9 中。

[0427] 图 17 显示在过程解释中参照的流程图，该过程在此实施例中用于验证设备认证信息已正确包括在 CE 设备中。

[0428] 对于在过程中包括的每个处理，作为与图 6 所示流程图中其对应物相同的处理，通过与对应物相同的步骤号进行表示，并且其解释将不提供或简化。

[0429] 步骤 90 到 106 与第一实施例中其相应的对应物相同。

[0430] 然而，在步骤 106 中，写入模块 30a 比较通过使用设备端验证散列函数 34 生成的

第一散列值与从管理服务器 7 收到的第一散列值，以便确定前者和后者是否彼此相等，并且将比较结果输出到认证信息写入验证模块 36。

[0431] 随后，在下一步骤 502 中，认证信息写入验证模块 36 从写入模块 30a 接收比较结果，并且也通过认证模块 20 获取设备 ID 41。随后，认证信息写入验证模块 36 将比较结果和设备 ID 41 经连接装置 10 输出到工厂系统。

[0432] 在步骤 504 中，工厂系统将产品序列号添加到已从认证信息写入验证模块 36 收到的比较结果和设备 ID 41，将产品序列号、比较结果和设备 ID 41 传送到管理服务器 7。

[0433] 在步骤 506 中，管理服务器 7 从工厂系统接收产品序列号、比较结果和设备 ID 41。随后，基于比较的结果，管理服务器 7 验证通过使用设备端验证散列函数 34 生成的第一散列值和从管理服务器 7 收到的第一散列值是否彼此相等，确认设备认证信息已包括在 CE 设备 9 中。

[0434] 剩余的步骤与第一实施例中其相应的对应物相同。也就是说，在步骤 134 中，管理服务器 7 通过将设备 ID 41 和产品序列号彼此相关联，将设备 ID 41 和产品序列号存储在存储器中。随后，在下一步骤 136 中，管理服务器 7 在接收的数据上添加日期，在带有日期的数据上添加做为秘密信息的签名，并将带有日期的数据传送到工厂系统。

[0435] 在工厂系统，验证签名以确认设备认证信息已正确包括在 CE 设备 9 中。

[0436] 如上所述，在该实施例的情况下，管理服务器 7 能够基于验证结果而确认设备认证信息已包括在 CE 设备 9 中。

[0437] 另外，由于管理服务器 7 不需要生成第二散列值，因此，管理服务器 7 承担的负荷量可减少。

[0438] 在此实施例的情况下，写入模块 30a 生成第一散列值。然而，要注意的是，也可以提供另一种配置，在该配置中，认证模块提供有设备端验证散列函数 34 以便允许认证模块生成第一散列值。在此配置中，认证信息写入验证模块 36 从证模块接收第一散列值和设备 ID，并验证收到的散列值与另一散列值相等。

[0439] 另外，也可提供一种配置，其中，认证信息写入验证模块 36 的功能包括在写入模块 30a 中。这种情况下，写入模块 30a 将验证结果传送到管理服务器 7。

图 1

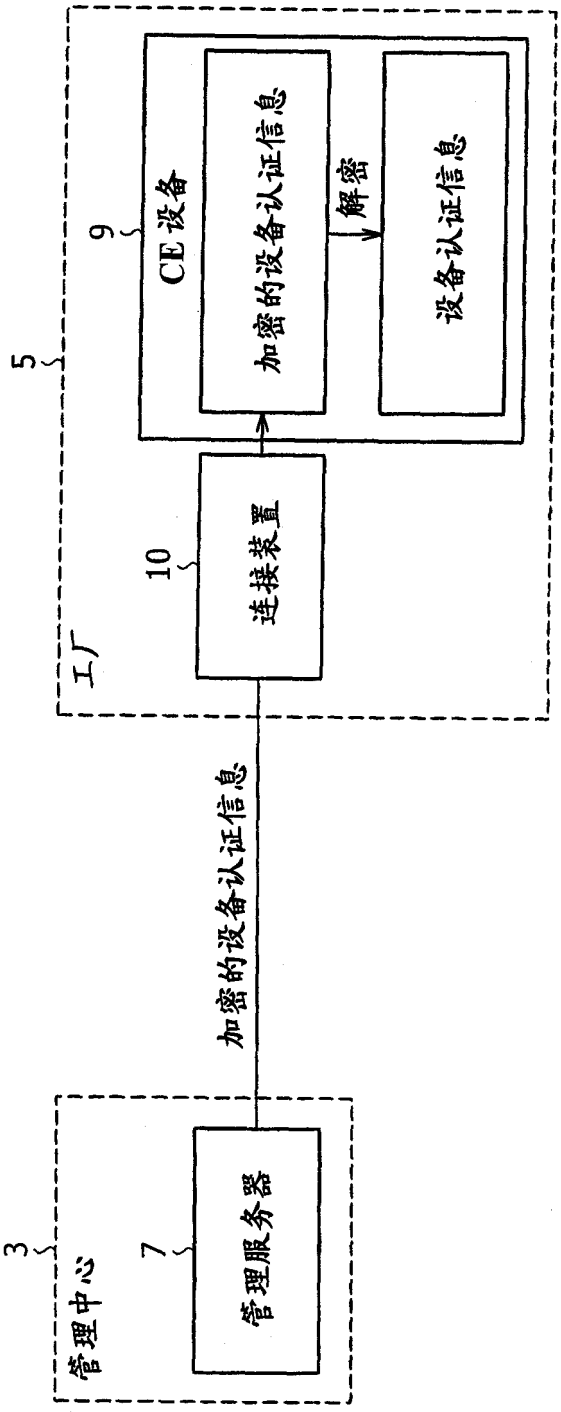

管理中心
3
管理服务器
7
加密的设备认证信息
工厂
5
连接装置
10
CE 设备
9
加密的设备认证信息
解密
设备认证信息

图 2

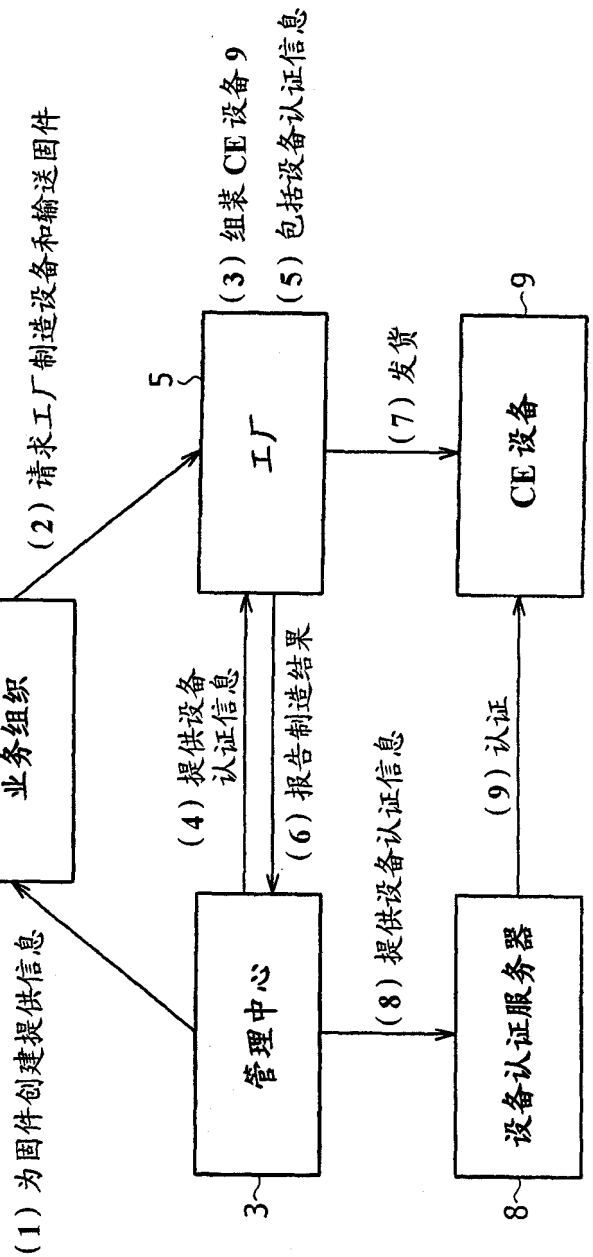
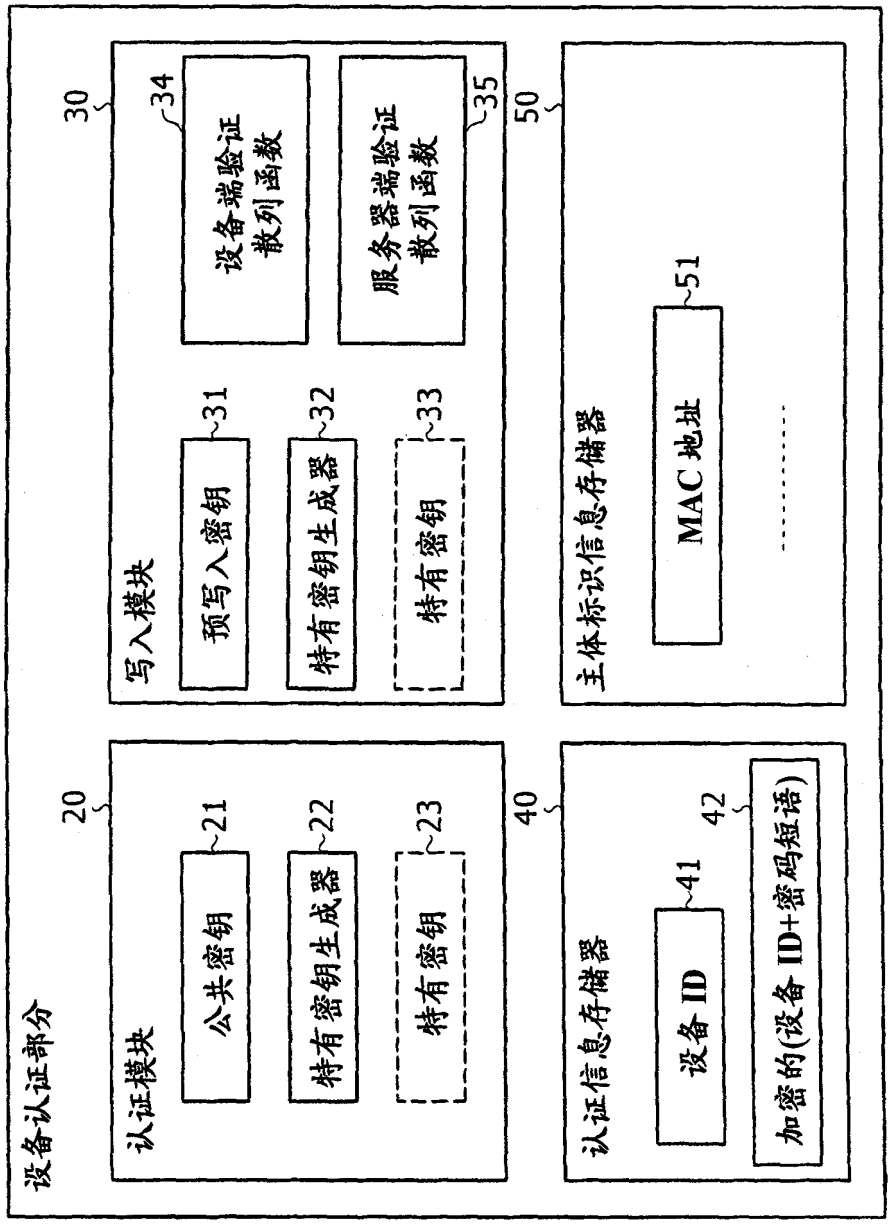

1
11
业务组织
(1) 为固件创建提供信息
(2) 请求工厂制造设备和输送固件
5
工厂
(3) 组装 CE 设备 9
(5) 包括设备认证信息
(4) 提供设备认证信息
(6) 报告制造结果
(7) 发货
9
CE 设备
管理中心
3
(8) 提供设备认证信息
(9) 认证
设备认证服务器
8

图 3


99
设备认证部分
20
认证模块
公共密钥
21
特有密钥生成器
22
特有密钥
23
30
写入模块
预写入密钥
31
特有密钥生成器
32
特有密钥
33
34
设备端验证散列函数
服务器端验证散列函数
35
40
认证信息存储器
设备 ID
41
加密的(设备 ID+密码短语)
42
50
主体标识信息存储器
MAC 地址
51
.....

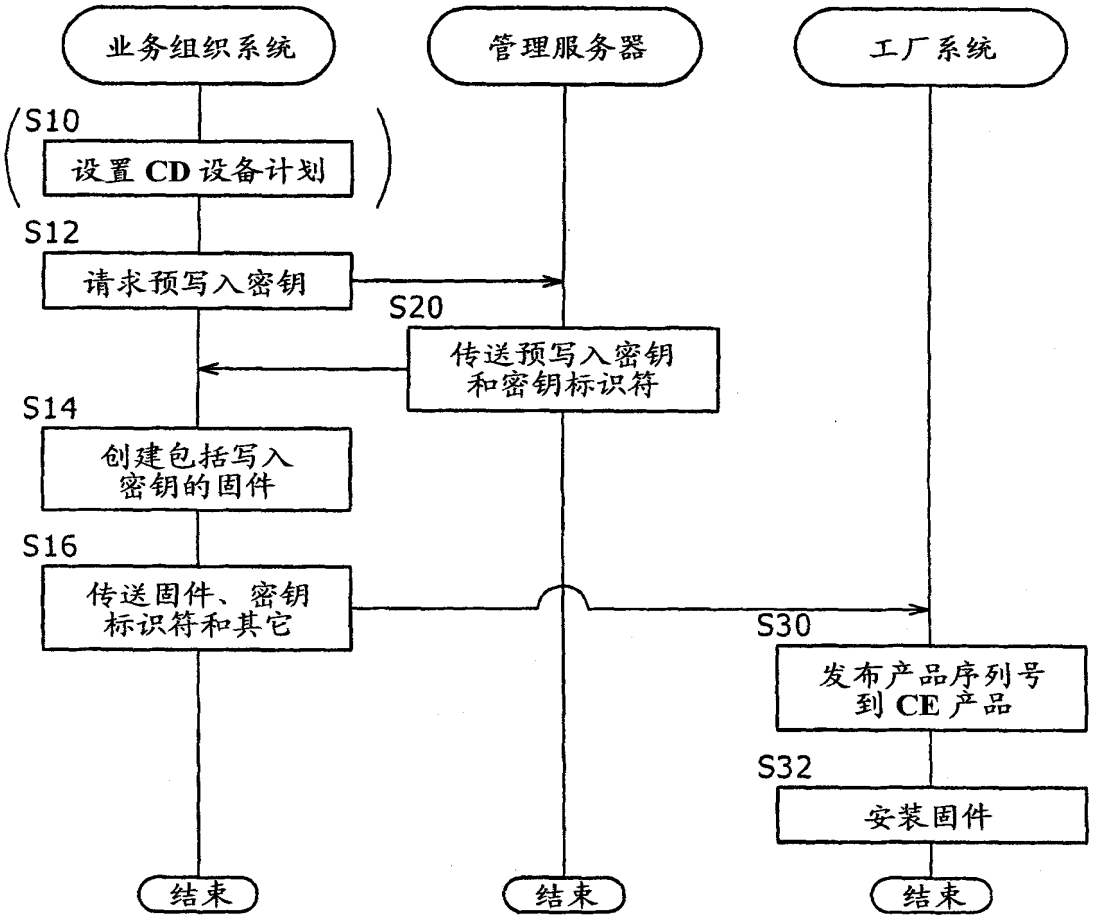

业务组织系统
管理服务器
工厂系统
S10
设置 CD 设备计划
S12
请求预写入密钥
S20
传送预写入密钥和密钥标识符
S14
创建包括写入密钥的固件
S16
传送固件、密钥标识符和其它
S30
发布产品序列号到 CE 产品
S32
安装固件
结束
结束
结束

图 4

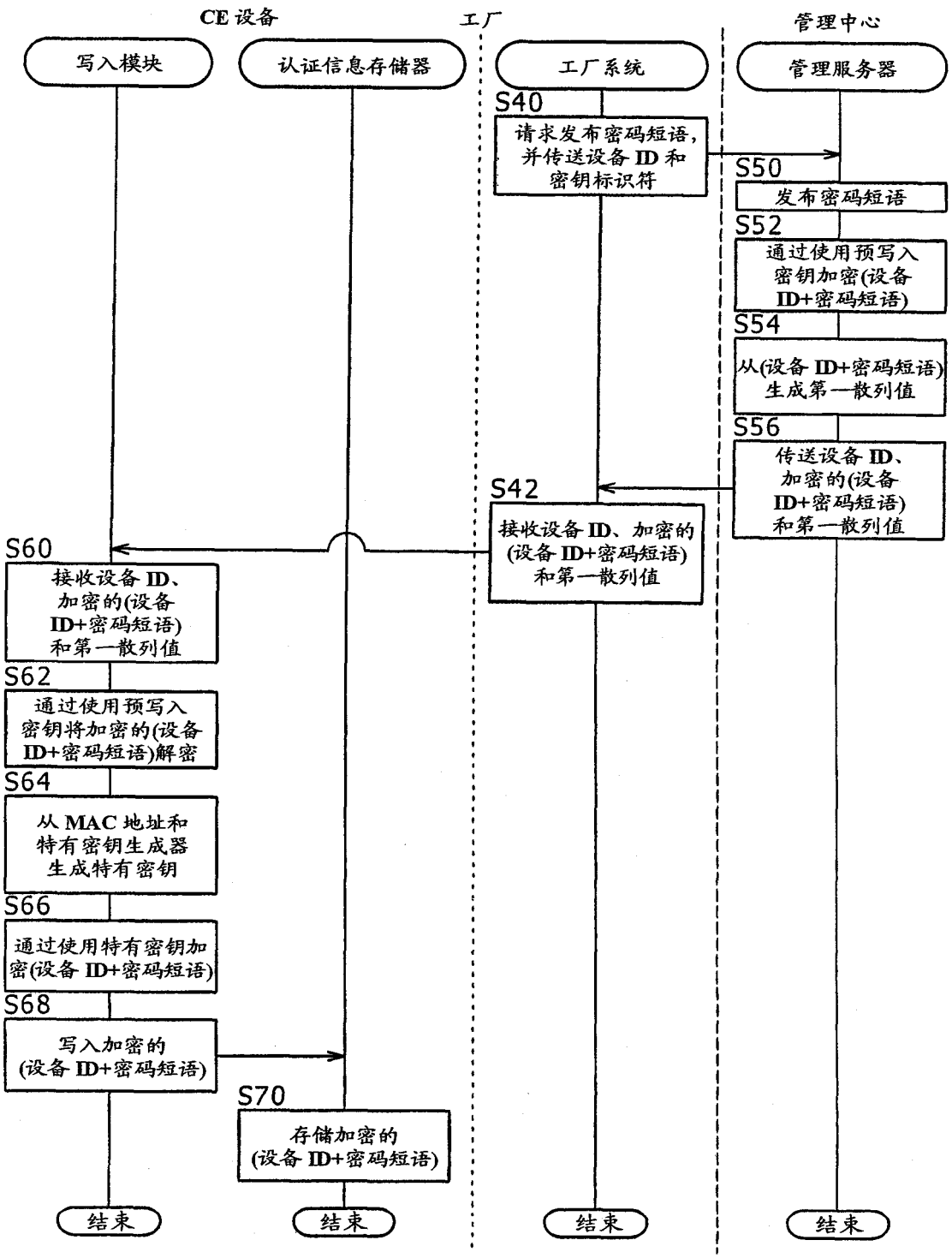

CE 设备
工厂
管理中心
写入模块
认证信息存储器
工厂系统
管理服务器
S40
请求发布密码短语，并传送设备 ID 和密钥标识符
S50
发布密码短语
S52
通过使用预写入密钥加密(设备 ID+密码短语)
S54
从(设备 ID+密码短语)生成第一散列值
S56
传送设备 ID、加密的(设备 ID+密码短语)和第一散列值
S42
接收设备 ID、加密的(设备 ID+密码短语)和第一散列值
S60
接收设备 ID、加密的(设备 ID+密码短语)和第一散列值
S62
通过使用预写入密钥将加密的(设备 ID+密码短语)解密
S64
从 MAC 地址和特有密钥生成器生成特有密钥
S66
通过使用特有密钥加密(设备 ID+密码短语)
S68
写入加密的(设备 ID+密码短语)
S70
存储加密的(设备 ID+密码短语)
结束
结束
结束
结束

图 5

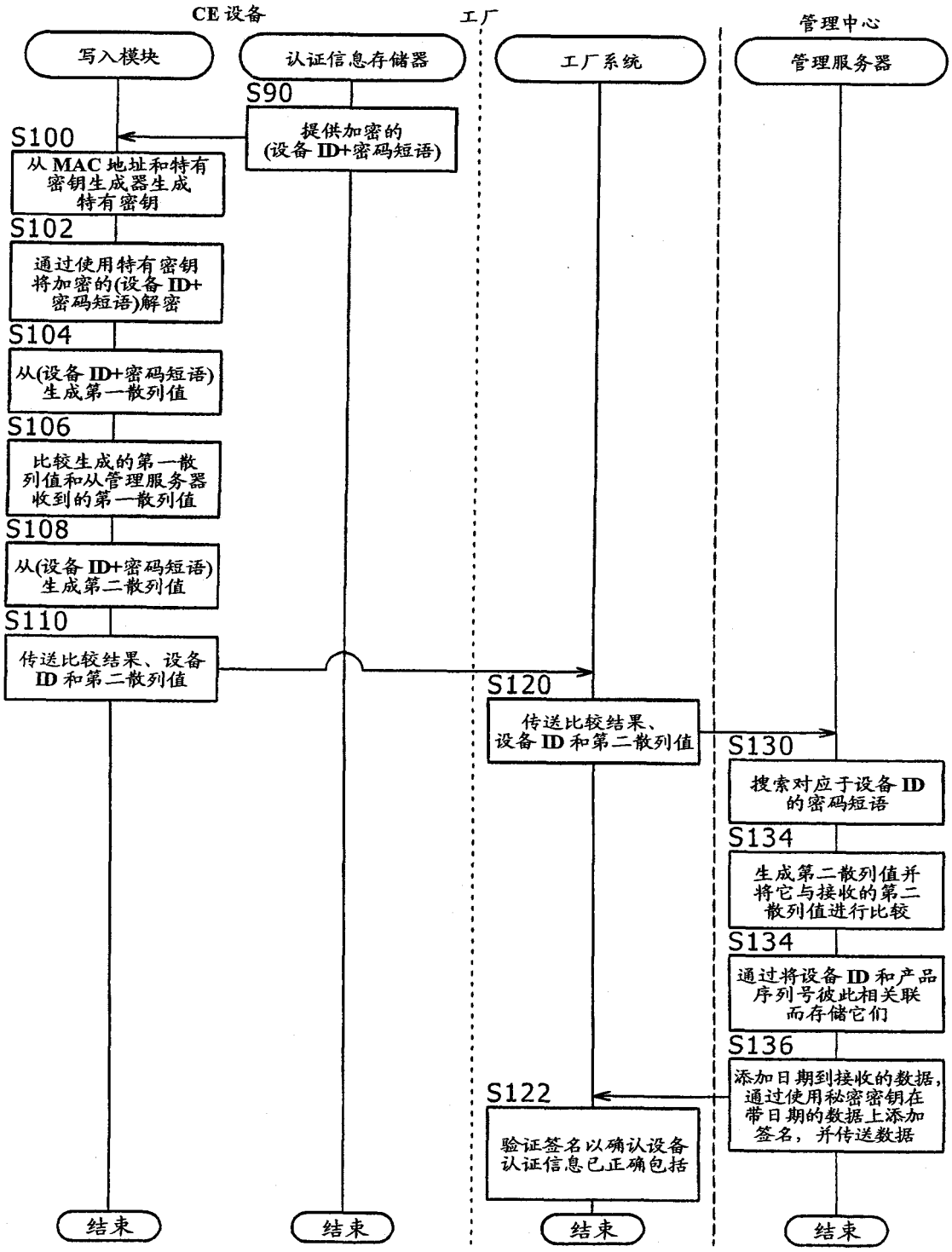

CE 设备
工厂
管理中心
写入模块
认证信息存储器
工厂系统
管理服务器
S90
提供加密的(设备 ID+密码短语)
S100
从 MAC 地址和特有密钥生成器生成特有密钥
S102
通过使用特有密钥将加密的(设备 ID+密码短语)解密
S104
从(设备 ID+密码短语)生成第一散列值
S106
比较生成的第一散列值和从管理服务器收到的第一散列值
S108
从(设备 ID+密码短语)生成第二散列值
S110
传送比较结果、设备 ID 和第二散列值
S120
传送比较结果、设备 ID 和第二散列值
S130
搜索对应于设备 ID 的密码短语
S134
生成第二散列值并将它与接收的第二散列值进行比较
S134
通过将设备 ID 和产品序列号彼此相关联而存储它们
S136
添加日期到接收的数据，通过使用秘密密钥在带日期的数据上添加签名，并传送数据
S122
验证签名以确认设备认证信息已正确包括
结束
结束
结束
结束

图 6

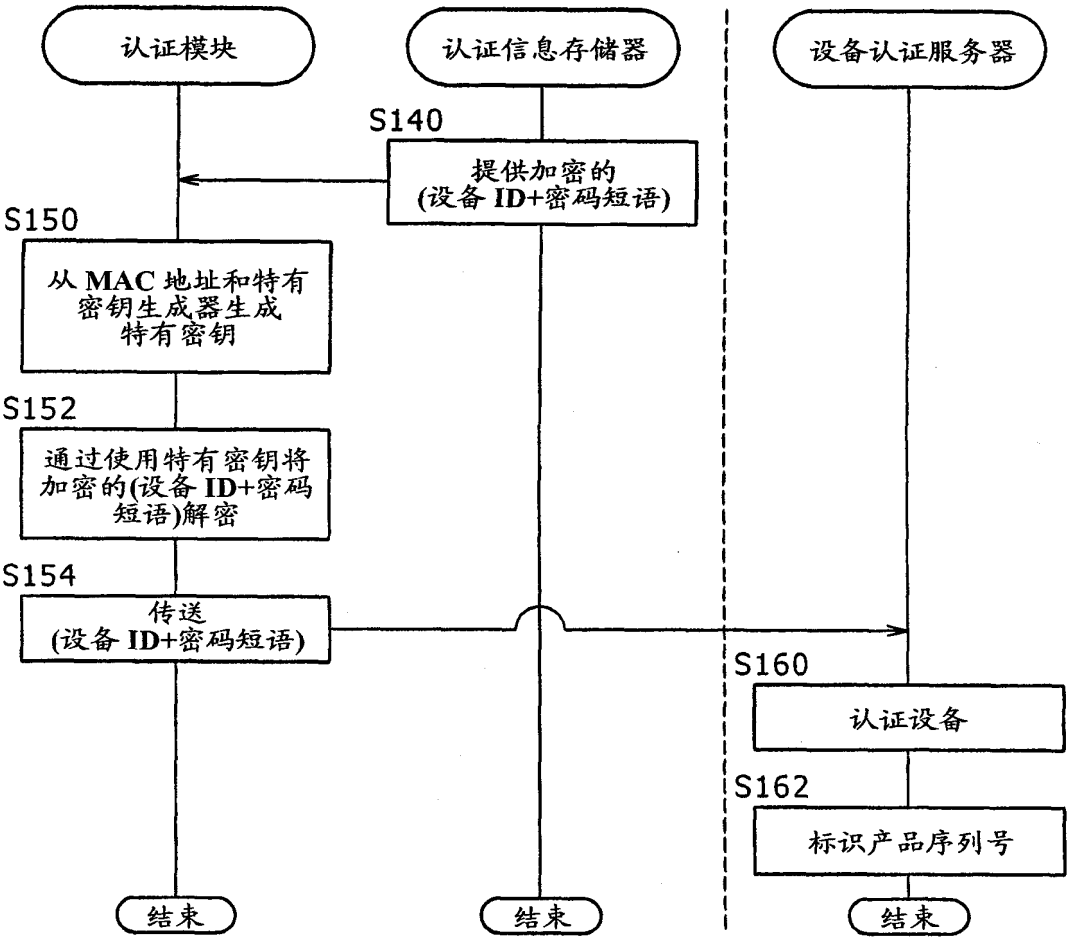

认证模块
认证信息存储器
设备认证服务器
S140
提供加密的
(设备 ID+密码短语)
S150
从 MAC 地址和特有
密钥生成器生成
特有密钥
S152
通过使用特有密钥将
加密的(设备 ID+密码
短语)解密
S154
传送
(设备 ID+密码短语)
S160
认证设备
S162
标识产品序列号
结束
结束
结束

图 7

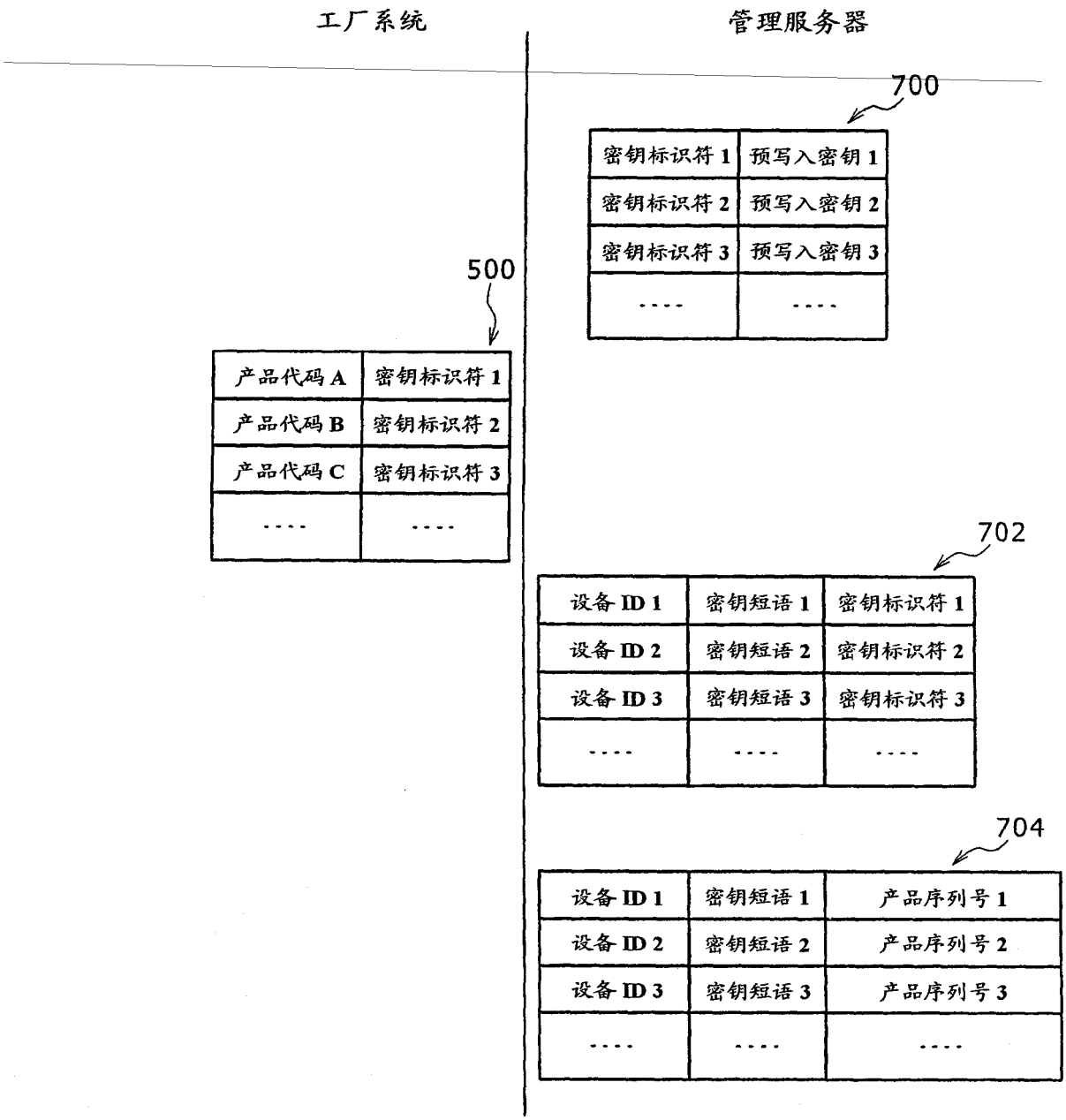

工厂系统
管理服务器
700
密钥标识符 1
预写入密钥 1
密钥标识符 2
预写入密钥 2
密钥标识符 3
预写入密钥 3
500
产品代码 A
密钥标识符 1
产品代码 B
密钥标识符 2
产品代码 C
密钥标识符 3
702
设备 ID 1
密钥短语 1
密钥标识符 1
设备 ID 2
密钥短语 2
密钥标识符 2
设备 ID 3
密钥短语 3
密钥标识符 3
704
设备 ID 1
密钥短语 1
产品序列号 1
设备 ID 2
密钥短语 2
产品序列号 2
设备 ID 3
密钥短语 3
产品序列号 3

图 8

图 9

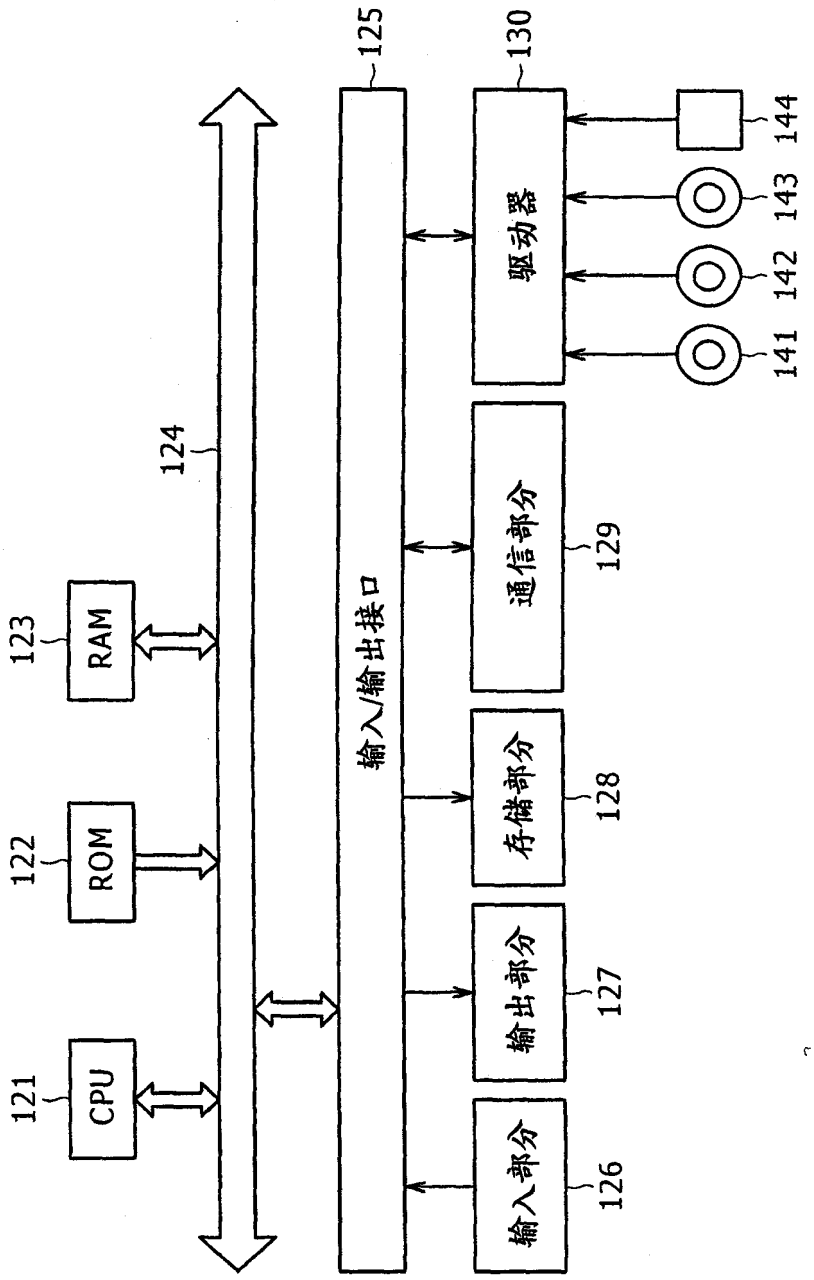
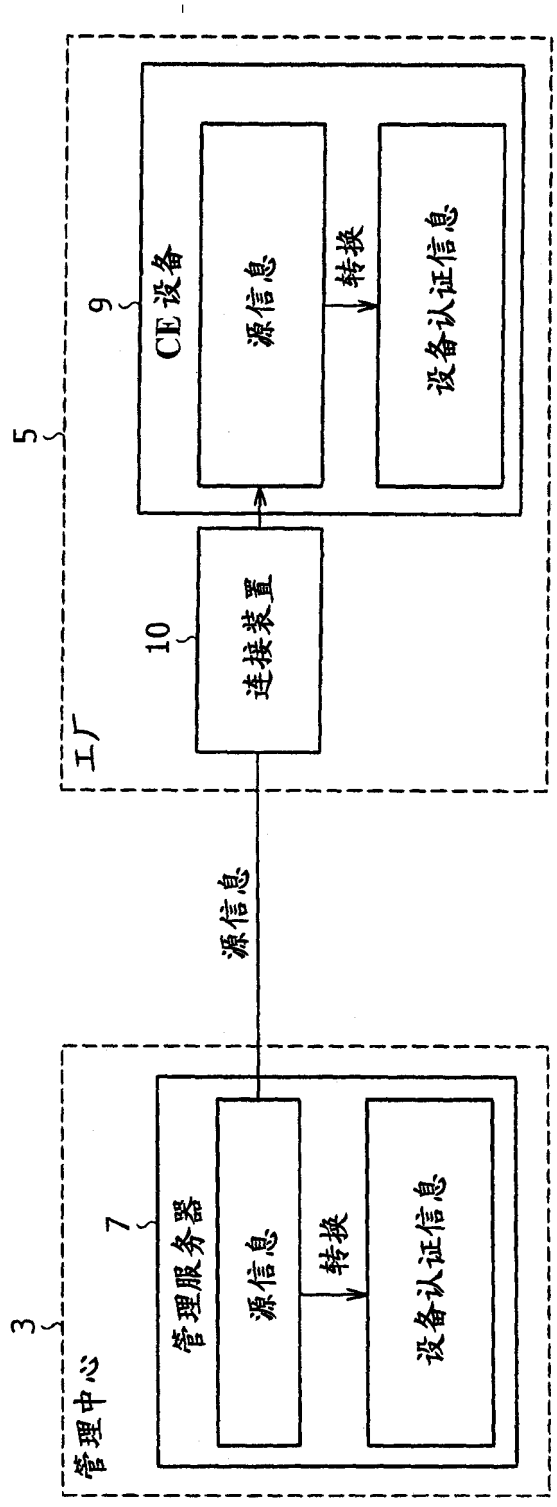

121
CPU
122
ROM
123
RAM
124
125
输入/输出接口
126
输入部分
127
输出部分
128
存储部分
129
通信部分
130
驱动器
141
142
143
144

图 10


管理中心
3
管理服务器
7
源信息
转换
设备认证信息
源信息
工厂
5
CE 设备
9
源信息
转换
设备认证信息
连接装置
10

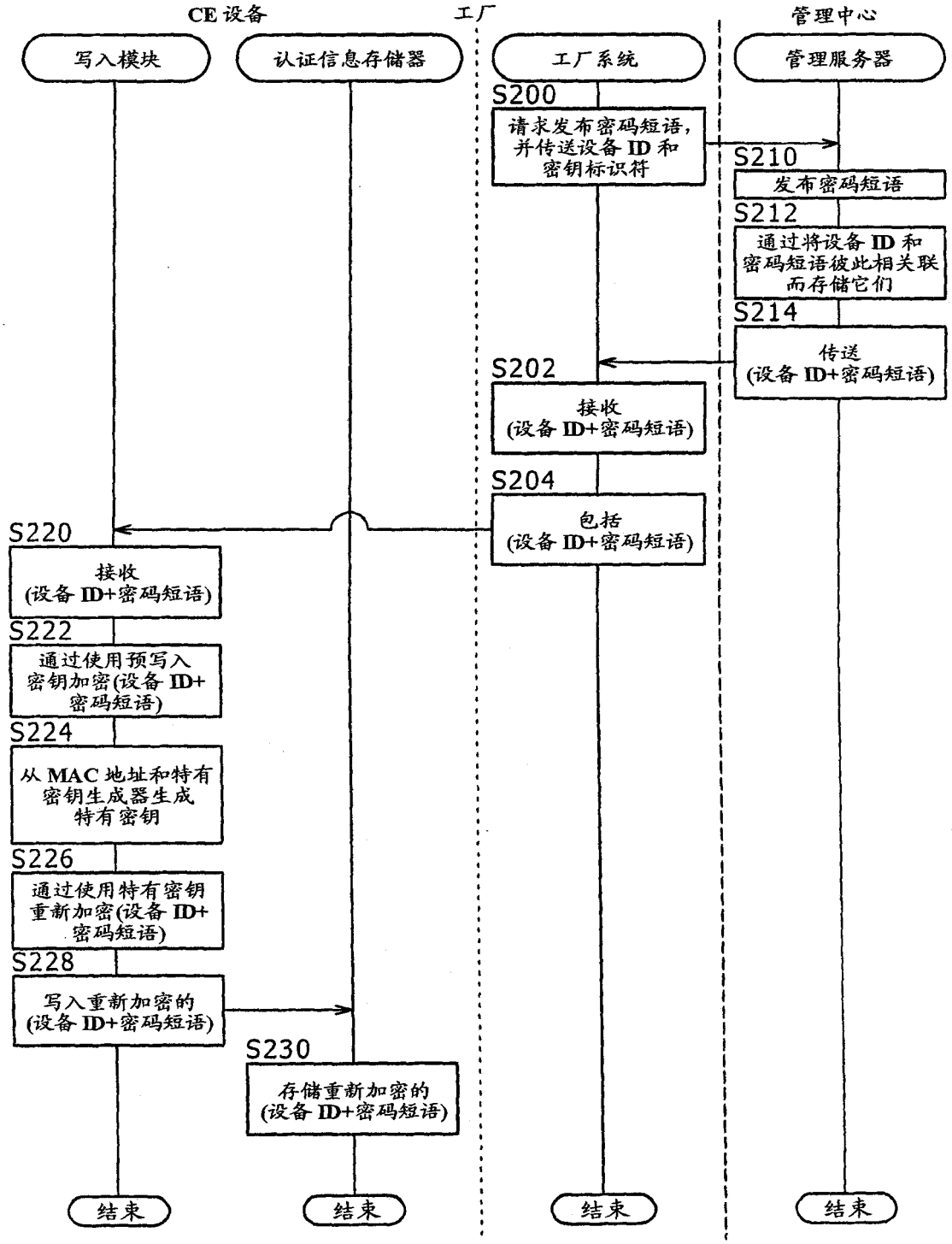

CE 设备
工厂
管理中心
写入模块
认证信息存储器
工厂系统
管理服务器
S200
请求发布密码短语，并传送设备 ID 和密钥标识符
S210
发布密码短语
S212
通过将设备 ID 和密码短语彼此相关联而存储它们
S214
传送
(设备 ID+密码短语)
S202
接收
(设备 ID+密码短语)
S204
包括
(设备 ID+密码短语)
S220
接收
(设备 ID+密码短语)
S222
通过使用预写入密钥加密(设备 ID+密码短语)
S224
从 MAC 地址和特有密钥生成器生成特有密钥
S226
通过使用特有密钥重新加密(设备 ID+密码短语)
S228
写入重新加密的
(设备 ID+密码短语)
S230
存储重新加密的
(设备 ID+密码短语)
结束
结束
结束
结束

图 11

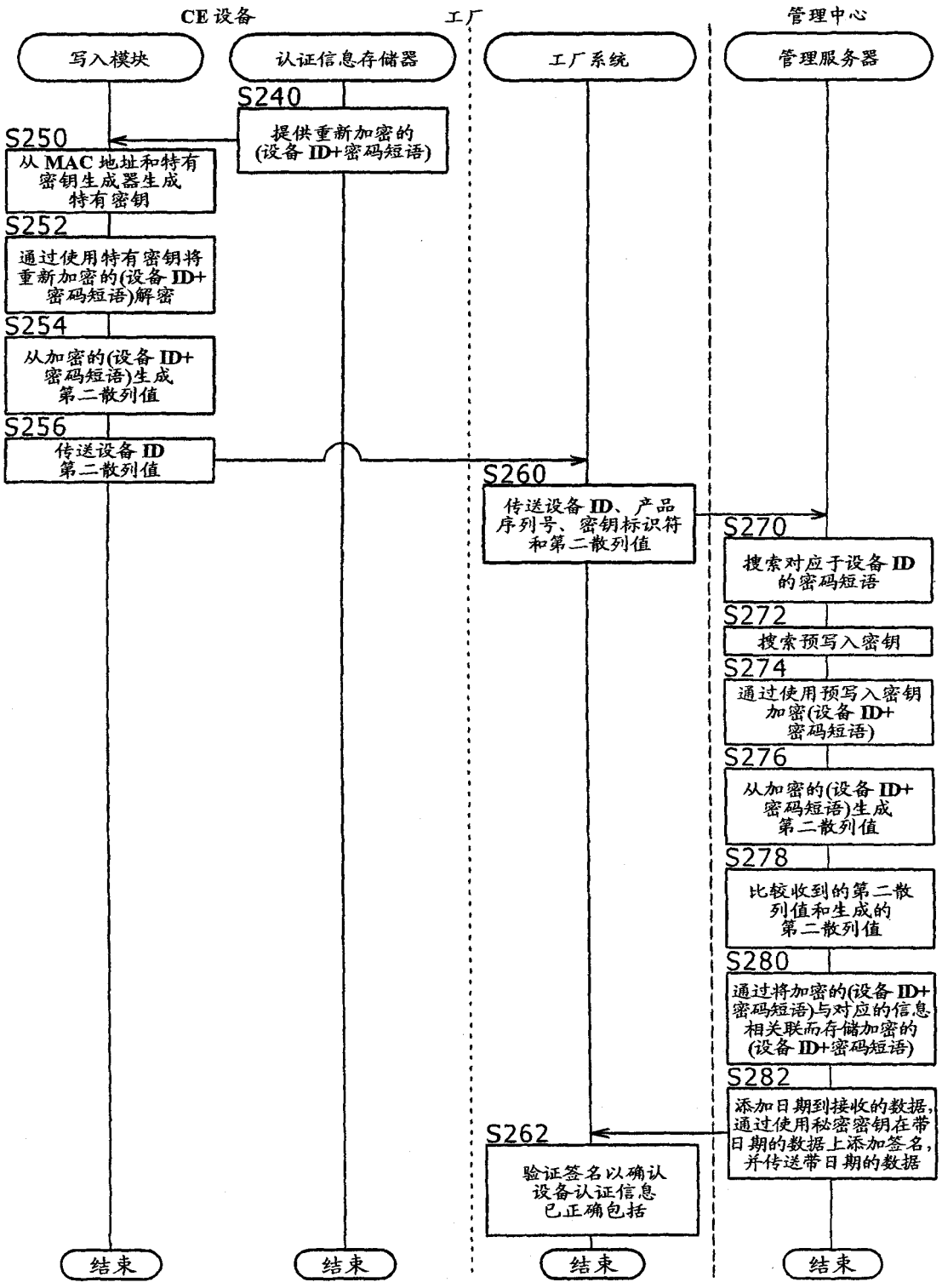

CE 设备
工厂
管理中心
写入模块
认证信息存储器
工厂系统
管理服务器
S240
提供重新加密的(设备 ID+密码短语)
S250
从 MAC 地址和特有密钥生成器生成特有密钥
S252
通过使用特有密钥将重新加密的(设备 ID+密码短语)解密
S254
从加密的(设备 ID+密码短语)生成第二散列值
S256
传送设备 ID 第二散列值
S260
传送设备 ID、产品序列号、密钥标识符和第二散列值
S270
搜索对应于设备 ID 的密码短语
S272
搜索预写入密钥
S274
通过使用预写入密钥加密(设备 ID+密码短语)
S276
从加密的(设备 ID+密码短语)生成第二散列值
S278
比较收到的第二散列值和生成的第二散列值
S280
通过将加密的(设备 ID+密码短语)与对应的信息相关联而存储加密的(设备 ID+密码短语)
S282
添加日期到接收的数据，通过使用秘密密钥在带日期的数据上添加签名，并传送带日期的数据
S262
验证签名以确认设备认证信息已正确包括
结束
结束
结束
结束

图 12

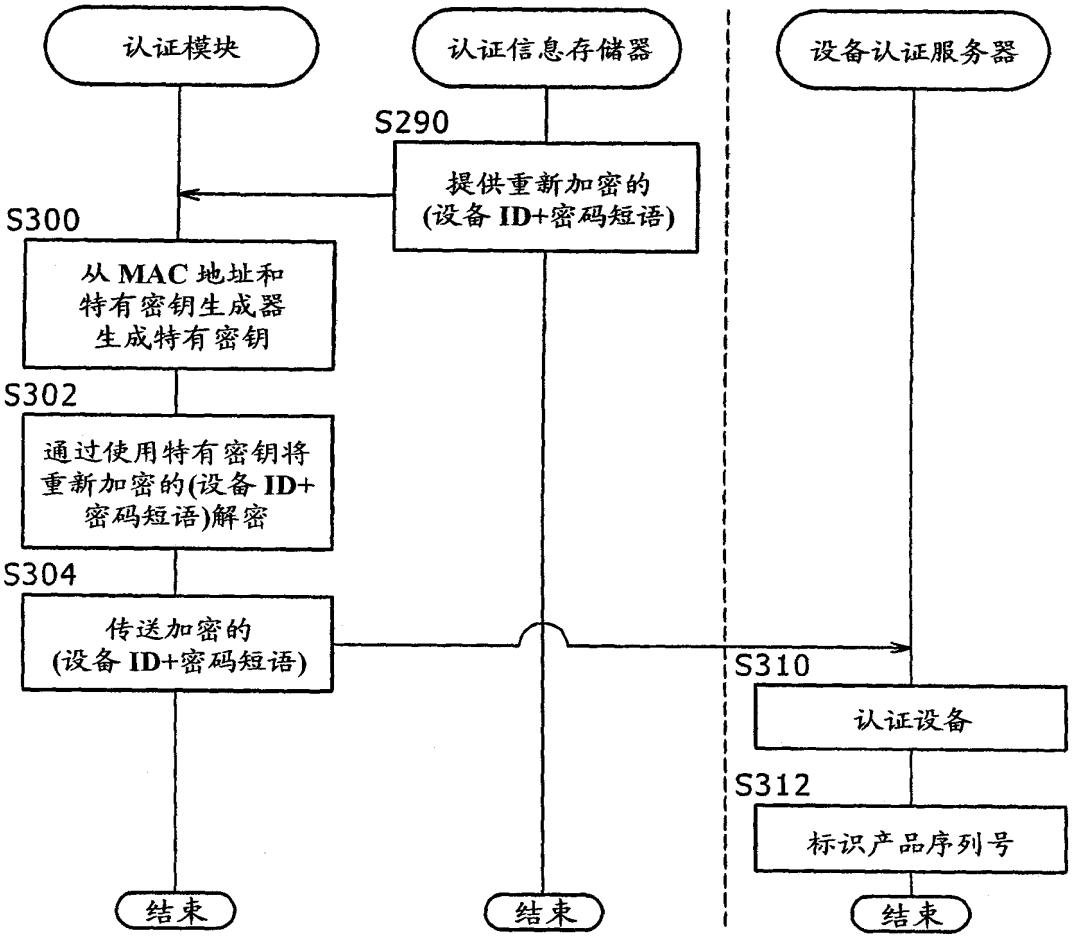

认证模块
认证信息存储器
设备认证服务器
S290
提供重新加密的
(设备 ID+密码短语)
S300
从 MAC 地址和
特有密钥生成器
生成特有密钥
S302
通过使用特有密钥将
重新加密的(设备 ID+
密码短语)解密
S304
传送加密的
(设备 ID+密码短语)
S310
认证设备
S312
标识产品序列号
结束
结束
结束

图 13

认证信息管理服务器

706

密钥标识符 1	预写入密钥 1
密钥标识符 2	预写入密钥 2
密钥标识符 3	预写入密钥 3
....	....

708

设备 ID 1	密钥短语 1
设备 ID 2	密钥短语 2
设备 ID 3	密钥短语 3
....	....

710

设备 ID 1	加密的（设备 ID 1+密码短语 1）	产品序列号 1	密钥标识符 1
设备 ID 2	加密的（设备 ID 2+密码短语 2）	产品序列号 2	密钥标识符 2
设备 ID 3	加密的（设备 ID 3+密码短语 3）	产品序列号 3	密钥标识符 3
....	....	....	....

图 14

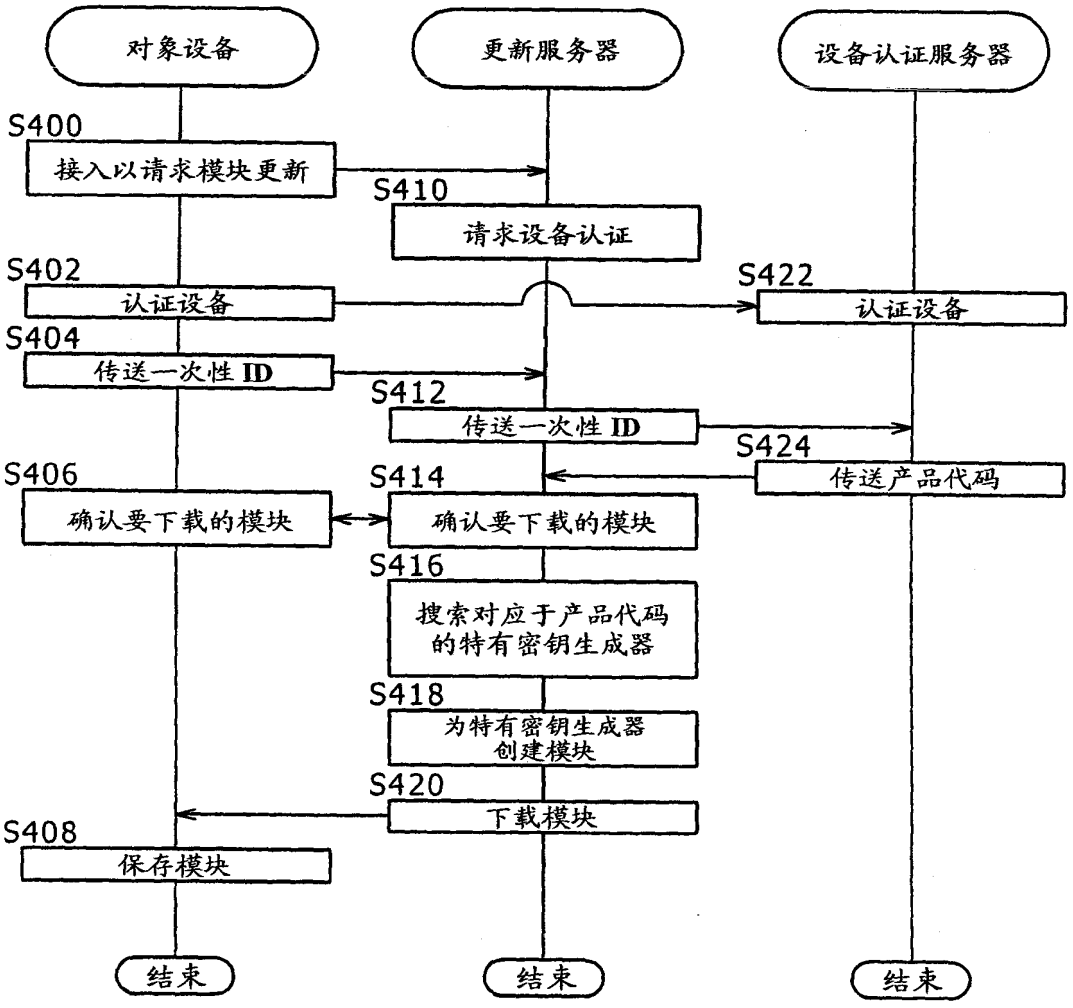
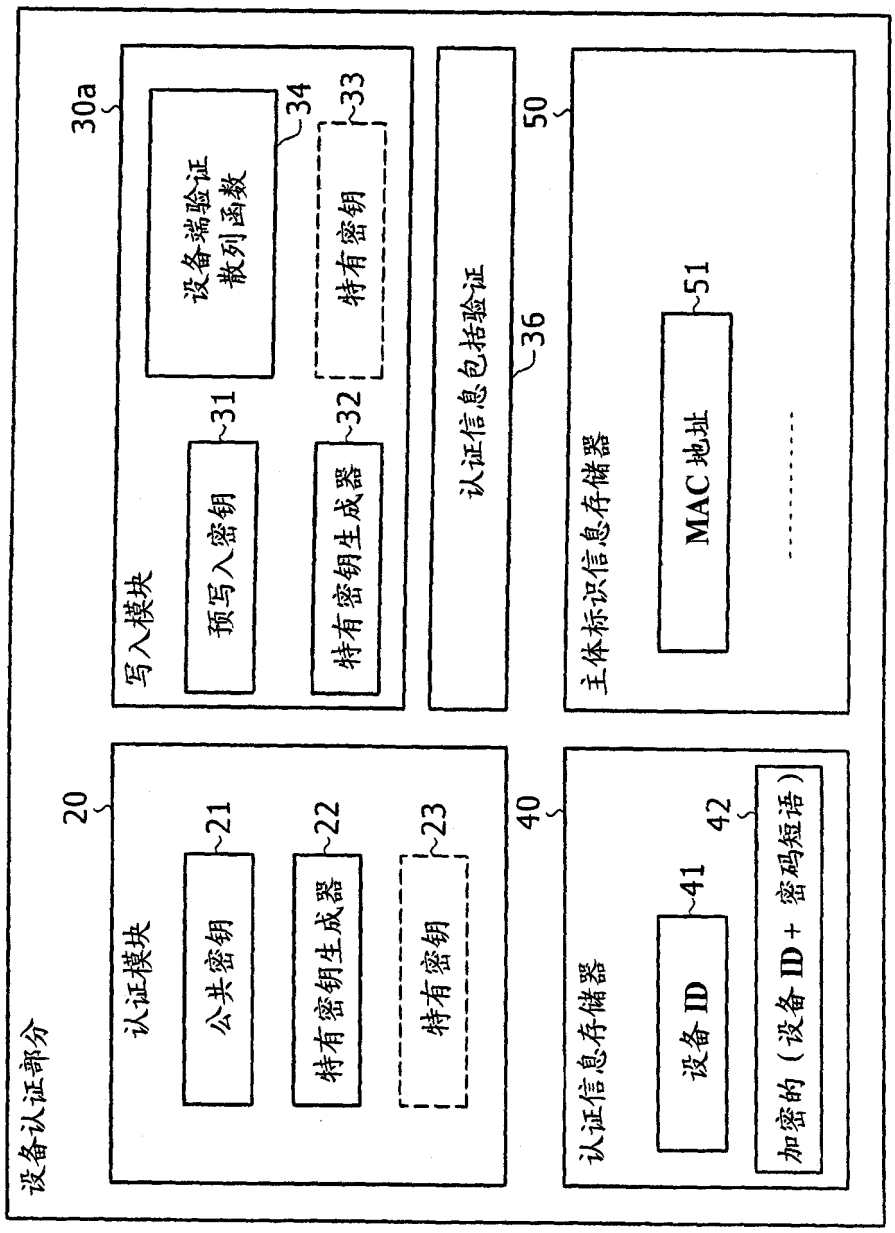

对象设备
更新服务器
设备认证服务器
S400
接入以请求模块更新
S410
请求设备认证
S402
认证设备
S422
认证设备
S404
传送一次性 ID
S412
传送一次性 ID
S424
传送产品代码
S406
确认要下载的模块
S414
确认要下载的模块
S416
搜索对应于产品代码的特有密钥生成器
S418
为特有密钥生成器创建模块
S420
下载模块
S408
保存模块
结束
结束
结束

图 15

图 16


99a
设备认证部分
20
认证模块
公共密钥
21
特有密钥生成器
22
特有密钥
23
30a
写入模块
预写入密钥
31
特有密钥生成器
32
特有密钥
33
设备端验证散列函数
34
认证信息包括验证
36
40
认证信息存储器
设备 ID
41
加密的（设备 ID + 密码短语）
42
50
主体标识信息存储器
MAC 地址
51
.....

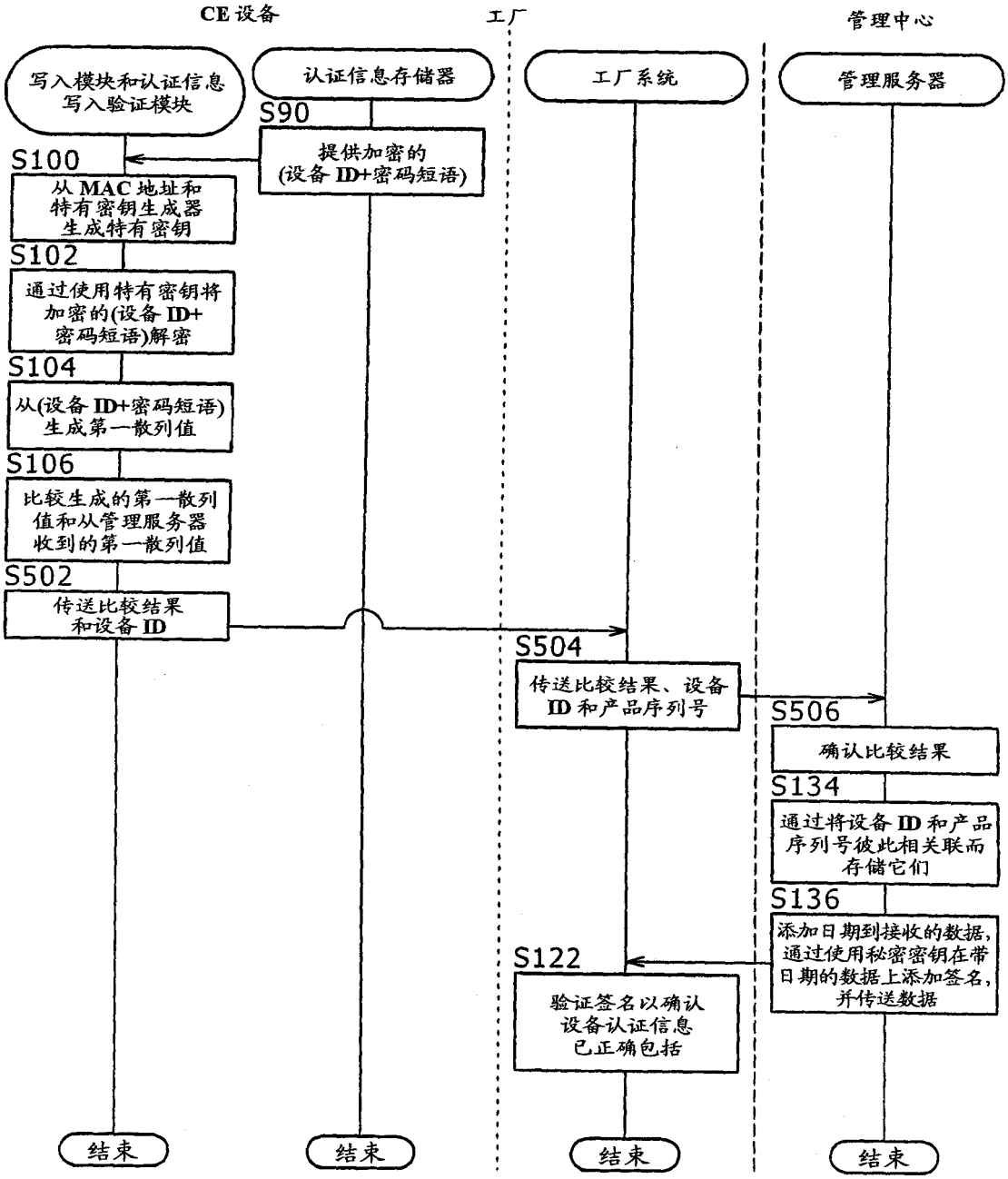

CE 设备
工厂
管理中心
写入模块和认证信息
写入验证模块
认证信息存储器
工厂系统
管理服务器
S90
提供加密的
(设备 ID+密码短语)
S100
从 MAC 地址和
特有密钥生成器
生成特有密钥
S102
通过使用特有密钥将
加密的(设备 ID+
密码短语)解密
S104
从(设备 ID+密码短语)
生成第一散列值
S106
比较生成的第一散列
值和从管理服务器
收到的第一散列值
S502
传送比较结果
和设备 ID
S504
传送比较结果、设备
ID 和产品序列号
S506
确认比较结果
S134
通过将设备 ID 和产品
序列号彼此相关联而
存储它们
S136
添加日期到接收的数据,
通过使用秘密密钥在带
日期的数据上添加签名,
并传送数据
S122
验证签名以确认
设备认证信息
已正确包括
结束
结束
结束
结束

图 17

图 18