(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117837125 A
(43)申请公布日 2024.04.05

(21)申请号 202180101740.2
(22)申请日 2021.09.13
(85)PCT国际申请进入国家阶段日
2024.02.22
(86)PCT国际申请的申请数据
PCT/JP2021/033437 2021.09.13
(87)PCT国际申请的公布数据
WO2023/037530 JA 2023.03.16
(71)申请人 GVE株式会社
地址 日本东京都
(72)发明人 高松圭太 房广治 日下部佑
(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 李逸雪
(51)Int.Cl.
H04L 9/32(2006.01)

权利要求书2页 说明书6页 附图4页

(54)发明名称

数据管理系统

(57)摘要

一种数据管理系统,具备客户装置、第一电子签名装置、数据管理装置、第二电子签名装置、数据保管装置以及第三电子签名装置,所述第一电子签名装置、所述第二电子签名装置以及所述第三电子签名装置中的至少一个电子签名装置是将加密密钥和权限建立对应地存储,且能够仅执行使用了所述加密密钥的处理中的与所述权限相应的处理的电子签名装置。

加密密钥	权限
客户装置的加密密钥	电子签名的赋予以及验证
数据管理装置的加密密钥	电子签名的验证
数据保管装置的加密密钥	电子签名的验证

CN 117837125 A

1.一种数据管理系统,具备客户装置、第一电子签名装置、数据管理装置、第二电子签名装置、数据保管装置以及第三电子签名装置,

所述客户装置生成第一请求消息,

所述客户装置对所述第一电子签名装置发送所述第一请求消息,

所述第一电子签名装置使用所述客户装置的加密密钥对所述第一请求消息附加电子签名,对所述客户装置发送附加了所述电子签名的所述第一请求消息,

所述客户装置生成包括附加了所述电子签名的所述第一请求消息的第二请求消息,

所述客户装置对所述第一电子签名装置发送所述第二请求消息,

所述第一电子签名装置使用所述客户装置的加密密钥对所述第二请求消息附加电子签名,对所述客户装置发送附加了所述电子签名的所述第二请求消息,

所述客户装置对所述数据管理装置发送附加了所述电子签名的所述第二请求消息,

所述数据管理装置对所述第二电子签名装置发送附加了所述电子签名的所述第二请求消息,

所述第二电子签名装置使用所述客户装置的加密密钥对附加于所述第二请求消息的电子签名进行验证,对所述数据管理装置发送所述验证的结果,

所述数据管理装置基于所述第二电子签名装置的验证的结果,对所述数据保管装置发送附加了所述电子签名的所述第一请求消息,

所述数据保管装置对所述第三电子签名装置发送附加了所述电子签名的所述第一请求消息,

所述第三电子签名装置使用所述客户装置的加密密钥对附加于所述第一请求消息的电子签名进行验证,对所述数据保管装置发送所述验证的结果,

所述数据保管装置基于所述第三电子签名装置的验证的结果,执行与所述第一请求消息相应的处理,生成第一响应消息,对所述第三电子签名装置发送所述第一响应消息,

所述第三电子签名装置使用所述数据保管装置的加密密钥对所述第一响应消息附加电子签名,对所述数据保管装置发送附加了所述电子签名的所述第一响应消息,

所述数据保管装置对所述数据管理装置发送附加了所述电子签名的所述第一响应消息,

所述数据管理装置执行与所述第二请求消息相应的处理,生成包括附加了所述电子签名的所述第一响应消息的第二响应消息,对所述第二电子签名装置发送所述第二响应消息,

所述第二电子签名装置使用所述数据管理装置的加密密钥对所述第二响应消息附加电子签名,对所述数据管理装置发送附加了所述电子签名的所述第二响应消息,

所述数据管理装置对所述客户装置发送附加了所述电子签名的所述第二响应消息,

所述客户装置对所述第一电子签名装置发送附加了所述电子签名的所述第二响应消息,

所述第一电子签名装置使用所述数据管理装置的加密密钥对附加于所述第二响应消息的电子签名进行验证,对所述客户装置发送该验证的结果,

所述客户装置对所述第一电子签名装置发送附加了所述电子签名的所述第一响应消息,

所述第一电子签名装置使用所述数据保管装置的加密密钥对附加于所述第一响应消息的电子签名进行验证,对所述客户装置发送该验证的结果,

所述客户装置基于所述第一电子签名装置的验证的结果,执行给定的处理。

2.根据权利要求1所述的数据管理系统,其中,

所述第一电子签名装置、所述第二电子签名装置以及所述第三电子签名装置中的至少一个电子签名装置是将加密密钥和权限建立对应地存储,且能够仅执行使用了所述加密密钥的处理中的与所述权限相应的处理的电子签名装置。

数据管理系统

技术领域

[0001] 本发明涉及数据的管理。

背景技术

[0002] 提出了以公钥方式赋予电子签名并进行验证的系统(参照专利文献1)。

[0003] 在先技术文献

[0004] 专利文献

[0005] 专利文献1:日本特开2008-140298号公报

发明内容

[0006] -发明所要解决的课题-

[0007] 本发明的一实施方式的目的在于,提供一种以秘钥方式赋予并验证电子签名的数据管理系统。

[0008] -用于解决课题的手段-

[0009] 本发明包括以下的一个实施方式。

[0010] 一种数据管理系统,是具备客户装置、第一电子签名装置、数据管理装置、第二电子签名装置、数据保管装置以及第三电子签名装置的数据管理系统,其中,所述第一电子签名装置、所述第二电子签名装置以及所述第三电子签名装置中的至少一个电子签名装置是将加密密钥和权限建立对应并存储,且能够仅执行使用了所述加密密钥的处理中的与所述权限相应的处理的电子签名装置。

[0011] -发明效果-

[0012] 根据本发明的一实施方式,能够提供以秘钥方式赋予并验证电子签名的数据管理系统。

附图说明

[0013] 图1是表示实施方式1所涉及的数据管理系统的结构例的图。

[0014] 图2是表示实施方式1所涉及的数据管理系统的动作例的图。

[0015] 图3A是表示第一电子签名装置中的密钥和权限的存储例的图。

[0016] 图3B是表示第二电子签名装置中的密钥和权限的存储例的图。

[0017] 图3C是表示第三电子签名装置中的密钥和权限的存储例的图。

[0018] 图4是表示实施方式2所涉及的数据管理系统的结构例的图。

具体实施方式

[0019] [实施方式1所涉及的数据管理系统]

[0020] 图1是表示实施方式1所涉及的数据管理系统的结构例的图。如图1所示,实施方式1所涉及的数据管理系统是具备客户装置、第一电子签名装置、数据管理装置、第二电子签

名装置、数据保管装置以及第三电子签名装置的数据管理系统。以下,对各装置进行说明。

[0021] (客户装置)

[0022] 客户装置是发送各种请求消息的装置。客户装置的一例包括膝上型计算机、智能手机、平板型计算机等。请求消息的一例包括数据包、信号等各种数据。后述的第一请求消息、第二请求消息是请求消息的一例。第一请求消息是对数据保管装置请求给定的处理的消息,第二请求消息是对数据管理装置请求给定的处理的消息。客户装置基于第一响应消息以及/或者第二响应消息执行给定的处理。基于第一响应消息的给定的处理的一例中包括取得数据显示、数据登记结果的显示、确认它们的处理。基于第二响应消息的给定的处理的一例中包括第一请求以及第二请求处理拒绝事由的显示、确认它们的处理(仅在数据管理装置或者数据保管装置中拒绝处理的情况)、消息发送接收历史的保存。

[0023] (数据管理装置)

[0024] 数据管理装置是基于从客户装置接收到的第二请求消息执行给定的处理,并对客户装置发送第二响应消息的装置。数据管理装置执行的给定的处理的一例包括数据登记、数据取得。数据管理装置的一例包括服务器计算机等。第二响应消息的一例包括数据登记响应、数据取得响应。

[0025] (数据保管装置)

[0026] 数据保管装置是基于从客户装置经由数据管理装置接收到的第一请求消息执行给定的处理,并经由数据管理装置对客户装置发送第二响应消息的装置。数据保管装置执行的给定的处理的一例中包括数据加密分布式写入、分布式数据解密读取。在数据保管装置的一例中包括分布式存储服务器(DSS:Distribute Storage Server)等。第一响应消息的一例中包括数据加密分布式写入响应、分布式数据解密读取响应。

[0027] (第一电子签名装置、第二电子签名装置、第三电子签名装置)

[0028] 第一电子签名装置、第二电子签名装置、第三电子签名装置是对请求消息、响应消息等消息赋予电子签名、以及对赋予给这些消息的电子签名进行验证的装置。第一电子签名装置、第二电子签名装置、第三电子签名装置例如能够使用HSM(硬件安全模块)等。第一电子签名装置是用于客户装置的电子签名装置。第二电子签名装置是用于数据管理装置的电子签名装置。第三电子签名装置是用于数据保管装置的电子签名装置。

[0029] 第一电子签名装置既可以经由网络与客户装置连接,也可以不经由网络而与客户装置连接,还可以内置于客户装置。在本实施方式中,第一电子签名装置经由网络与客户装置连接。

[0030] 第二电子签名装置可以经由网络与数据管理装置连接,也可以不经由网络与数据管理装置连接,还可以内置于数据管理装置。在本实施方式中,第二电子签名装置不经由网络而与数据管理装置连接。

[0031] 第三电子签名装置可以经由网络与数据保管装置连接,也可以不经由网络而与数据保管装置连接,还可以内置于数据保管装置。在本实施方式中,第三电子签名装置不经由网络地与数据保管装置连接。

[0032] 图3A是表示第一电子签名装置中的密钥和权限的存储例的图。图3B是表示第二电子签名装置中的密钥和权限的存储例的图。图3C是表示第三电子签名装置中的密钥和权限的存储例的图。如图3A、图3B、图3C所示,第一电子签名装置、第二电子签名装置以及第三电

子签名装置中的至少一个电子签名装置(在本实施方式中全部电子签名装置)是将加密密钥与权限建立对应地存储,且能够仅执行使用了加密密钥的处理中的与权限相应的处理的电子签名装置。

[0033] 作为电子签名装置,已知基于公钥方式进行电子签名的生成·验证的装置。

[0034] 但是,在公钥方式的情况下,存在公钥和秘钥,公钥非常长(例:2048比特)。

[0035] 另一方面,在秘钥方式的情况下,用秘钥(例:256比特)进行加密和验证。因此,在秘钥方式的情况下,不使用长的公钥即可,因此能够缩短电子签名的生成·赋予、验证的时间。不过,在采用秘钥方式的情况下,必须在多个电子签名装置之间共享加密密钥(秘钥)。因此,即使是仅进行由某个加密密钥生成的电子签名的验证的电子签名装置,也能够使用该加密密钥直到生成电子签名,存在安全上的问题。例如,在上述示例中,除了客户装置的加密密钥之外,第一电子签名装置还具有数据管理装置、数据保管装置的加密密钥。但是,在第一电子签名装置中,数据管理装置、数据保管装置的加密密钥只不过用于电子签名的验证。然而,第一电子签名装置能够使用数据管理装置、数据保管装置的加密密钥来生成电子签名。换言之,客户装置能够使用第一电子签名装置冒充数据管理装置、数据保管装置。

[0036] 因而,在本实施方式中,第一电子签名装置、第二电子签名装置以及第三电子签名装置采用秘钥方式,在这些电子签名装置之间共享加密密钥(秘钥)。不过,在本实施方式中,为了不产生安全上的问题,对共享的多个加密密钥(秘钥)赋予权限,第一电子签名装置、第二电子签名装置、以及第三电子签名装置只能在与该权限相应的处理中使用多个加密密钥(秘钥)。这样一来,能够确保安全,并且能够缩短电子签名的生成·赋予、验证的时间。例如,如果是第一电子签名装置,如图3A所示,不仅具有客户装置的加密密钥,还具有数据管理装置、数据保管装置的加密密钥。但是,对客户装置的加密密钥给予赋予以及验证的权限,对其他装置的加密密钥仅给予验证的权限。这样一来,第一电子签名装置能够使用客户装置的加密密钥来执行电子签名的赋予以及验证这双方,而使用其他装置的加密密钥仅能够执行电子签名的验证。

[0037] 在本实施方式中,为了充分确保安全,第一电子签名装置、第二电子签名装置、以及第三电子签名装置都是将加密密钥与权限建立对应地存储,且能够仅执行使用了加密密钥的处理中的与权限相应的处理的电子签名装置。

[0038] 加密密钥的比特数例如为128、256。加密密钥用于电子签名的赋予和验证双方。对于电子签名的赋予、验证,能够使用AES方式或其他方式。

[0039] 权限的一例包括“能够进行电子签名的赋予以及验证”、”仅能够进行电子签名的验证”等,除此之外,还包括“仅在给定的情况下能够进行电子签名的赋予”、“仅在给定的情况下能够进行电子签名的验证”、“电子签名的验证能够在任何时候进行,但电子签名的赋予能够仅在给定的情况下进行”等。

[0040] (动作例)

[0041] 图2是表示实施方式1所涉及的数据管理系统的动作例的图。以下,参照图2说明实施方式1所涉及的数据管理系统的动作例。另外,在本说明书中,有时将“赋予”电子签名称为“附加”电子签名。

[0042] (步骤1)

[0043] 首先,客户装置生成第一请求消息。

[0044] (步骤2)

[0045] 接下来,客户装置对第一电子签名装置发送第一请求消息。

[0046] (步骤3)

[0047] 接下来,第一电子签名装置使用客户装置的加密密钥对第一请求消息附加电子签名,对客户装置发送附加了电子签名的第一请求消息。

[0048] (步骤4)

[0049] 接下来,客户装置生成包括附加了电子签名的第一请求消息的第二请求消息。

[0050] (步骤5)

[0051] 接下来,客户装置对第一电子签名装置发送第二请求消息。

[0052] (步骤6)

[0053] 接下来,第一电子签名装置使用客户装置的加密密钥对第二请求消息附加电子签名,对客户装置发送附加了电子签名的第二请求消息。

[0054] (步骤7)

[0055] 接下来,客户装置对数据管理装置发送附加了电子签名的第二请求消息。

[0056] (步骤8)

[0057] 接下来,数据管理装置对第二电子签名装置发送附加了电子签名的第二请求消息。

[0058] (步骤9)

[0059] 接下来,第二电子签名装置使用客户装置的加密密钥对附加于第二请求消息的电子签名进行验证,对数据管理装置发送验证的结果。

[0060] (步骤10)

[0061] 接下来,数据管理装置基于第二电子签名装置的验证的结果,对数据保管装置发送附加了电子签名的第一请求消息。

[0062] (步骤11)

[0063] 接下来,数据保管装置对第三电子签名装置发送附加了电子签名的第一请求消息。

[0064] (步骤12)

[0065] 接下来,第三电子签名装置使用客户装置的加密密钥对附加于第一请求消息的电子签名进行验证,对数据保管装置发送验证的结果。

[0066] (步骤13)

[0067] 接下来,数据保管装置基于第三电子签名装置的验证的结果,执行与第一请求消息相应的处理。

[0068] (步骤14)

[0069] 接下来,数据保管装置生成第一响应消息。

[0070] (步骤15)

[0071] 接下来,数据保管装置对第三电子签名装置发送第一响应消息。

[0072] (步骤16)

[0073] 接下来,第三电子签名装置使用数据保管装置的加密密钥对第一响应消息附加电子签名,对数据保管装置发送附加了电子签名的第一响应消息。

[0074] (步骤17)

[0075] 接下来,数据保管装置对数据管理装置发送附加了电子签名的第一响应消息。

[0076] (步骤18)

[0077] 接下来,数据管理装置执行与第二请求消息相应的处理。

[0078] (步骤19)

[0079] 接下来,数据管理装置生成包括附加了电子签名的第一响应消息的第二响应消息。

[0080] (步骤20)

[0081] 接下来,数据管理装置对第二电子签名装置发送第二响应消息。

[0082] (步骤21)

[0083] 接下来,第二电子签名装置使用数据管理装置的加密密钥对第二响应消息附加电子签名,对数据管理装置发送附加了电子签名的第二响应消息。

[0084] (步骤22)

[0085] 接下来,数据管理装置对客户装置发送附加了电子签名的第二响应消息。

[0086] (步骤23)

[0087] 接下来,客户装置对第一电子签名装置发送附加了电子签名的第二响应消息。

[0088] (步骤24)

[0089] 接下来,第一电子签名装置使用数据管理装置的加密密钥对附加于第二响应消息的电子签名进行验证,对客户装置发送该验证的结果。

[0090] (步骤25)

[0091] 接下来,客户装置对第一电子签名装置发送附加了电子签名的第一响应消息。

[0092] (步骤26)

[0093] 接下来,第一电子签名装置使用数据保管装置的加密密钥对附加于第一响应消息的电子签名进行验证,对客户装置发送该验证的结果。

[0094] (步骤27)

[0095] 接下来,客户装置基于验证的结果执行给定的处理。

[0096] 根据以上说明的实施方式1,能够提供以秘钥方式(在多个电子签名装置之间共享加密密钥的方式)赋予电子签名并进行验证的数据管理系统。此外,根据实施方式1,能够提供尽管在多个电子签名装置之间共享加密密钥,但防止了某个装置(例:客户装置)冒充其他装置(例:数据管理装置、数据保管装置)的安全高的数据管理系统。此外,通过设定各种条件作为与加密密钥建立对应的权限,客户装置、数据管理装置、数据保管装置仅利用在数据管理系统上允许的电子签名的赋予、验证,虽然是秘钥方式(在多个电子签名装置之间共享加密密钥的方式),但能够进行严格地管理的电子签名的运用。

[0097] [实施方式2所涉及的数据管理系统]

[0098] 图4是表示实施方式2所涉及的数据管理系统的结构例的图。如图4所示,实施方式2所涉及的数据管理系统在密钥管理装置与第一电子签名装置、第二电子签名装置以及第三电子签名装置连接这一点上与实施方式1所涉及的数据管理系统不同。如上所述,在第一电子签名装置、第二电子签名装置以及第三电子签名装置中,共享客户装置、数据管理装置以及数据保管装置的加密密钥。密钥管理装置是将不同的权限与这些共享的加密密钥建立

对应并对各电子签名装置进行设定的装置。这样一来,例如在一个装置新追加了签名密钥时,能够向其他装置分发具有用于验证由该签名密钥生成的签名的适当的权限的密钥。密钥管理装置可以经由网络与第一电子签名装置、第二电子签名装置以及第三电子签名装置连接,也可以不经由网络地与第一电子签名装置、第二电子签名装置以及第三电子签名装置连接。在本实施方式中,密钥管理装置不经由网络地与第一电子签名装置、第二电子签名装置以及第三电子签名装置连接。

[0099] 以下,对使用了实施方式1、2的数据管理系统的一例进行说明。

[0100] 实施例1

[0101] 实施方式1、2所涉及的数据管理系统例如能够用于疫苗的接种证书(例:疫苗护照)的管理。在这种情况下,例如,客户装置的一例包括由医院、接种了疫苗的人、机场的海关、游乐园、餐饮店等使用的装置。医院使用医院管理的装置,在数据保管装置中保管疫苗的接种证书。此外,接种了疫苗的人、机场的海关、游乐园、餐饮店等能够使用各自管理的装置,将保管于数据保管装置中的疫苗的接种证书显示或印刷在客户装置的画面中。

[0102] 实施例2

[0103] 实施方式1、2所涉及的数据管理系统例如能够用于不动产登记。在这种情况下,例如,客户装置的一例包括由登记处、法人、个人、金融机构等使用的装置。登记处使用自己的装置将与不动产登记相关的数据保管于数据保管装置。此外,法人、个人、金融机构等能够使用各自管理的装置,将保管于数据保管装置中的与不动产登记相关的数据显示或印刷在客户装置的画面中。

[0104] 实施例3

[0105] 实施方式1、2所涉及的数据管理系统例如能够用于公司注册。在这种情况下,例如,客户装置用于注册机构、法人、个人、金融机构等。注册机构使用客户装置,将与公司注册相关的数据保管于数据保管装置。此外,法人、个人、金融机构等能够使用客户装置,将保管于数据保管装置中的与公司注册相关的数据显示或印刷在客户装置的画面中。

[0106] 以上,对实施例进行了说明,但实施方式1、2所涉及的数据保管系统能够用于其他各种数据的保管。

[0107] 以上,对实施方式进行了说明,但本发明不受这些说明的任何限定。

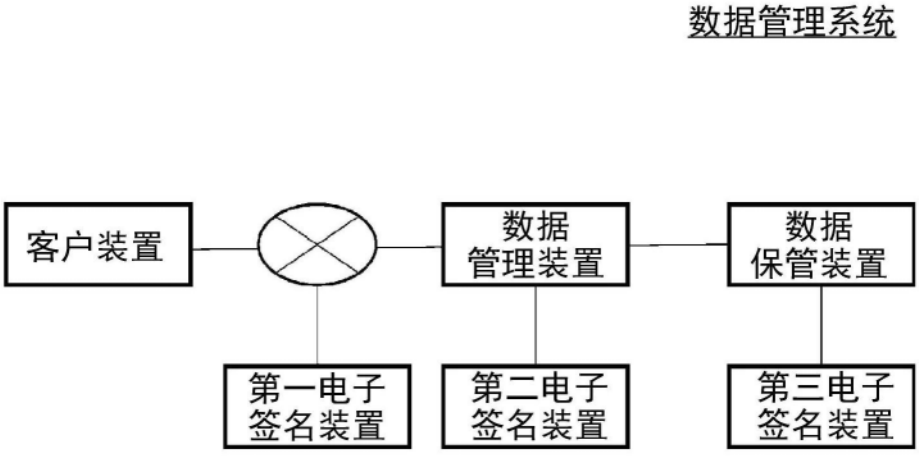

图1

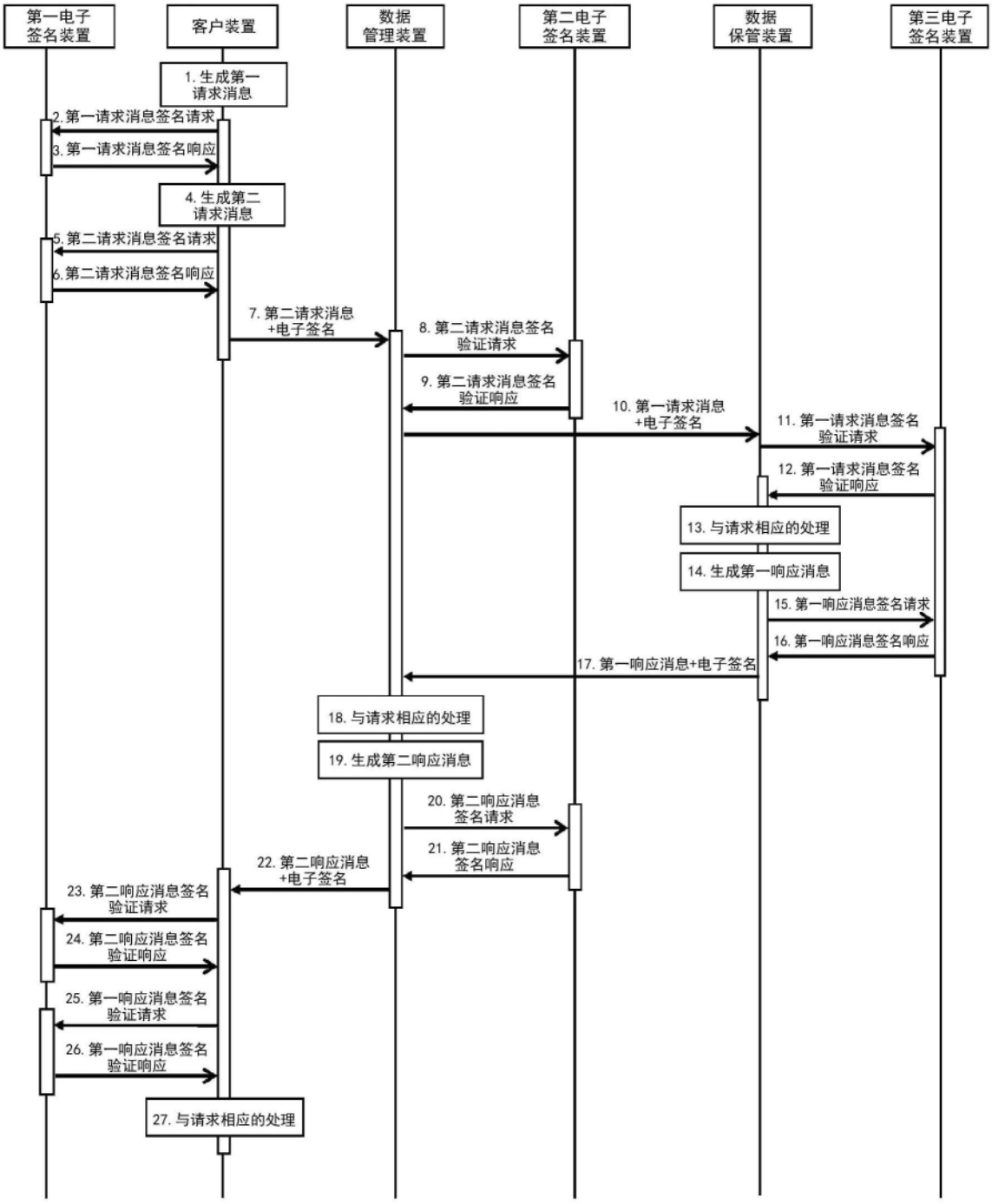
第一电子签名装置
客户装置
数据管理装置
第二电子签名装置
数据保管装置
第三电子签名装置
1. 生成第一请求消息
2. 第一请求消息签名请求
3. 第一请求消息签名响应
4. 生成第二请求消息
5. 第二请求消息签名请求
6. 第二请求消息签名响应
7. 第二请求消息+电子签名
8. 第二请求消息签名验证请求
9. 第二请求消息签名验证响应
10. 第一请求消息+电子签名
11. 第一请求消息签名验证请求
12. 第一请求消息签名验证响应
13. 与请求相应的处理
14. 生成第一响应消息
15. 第一响应消息签名请求
16. 第一响应消息签名响应
17. 第一响应消息+电子签名
18. 与请求相应的处理
19. 生成第二响应消息
20. 第二响应消息签名请求
21. 第二响应消息签名响应
22. 第二响应消息+电子签名
23. 第二响应消息签名验证请求
24. 第二响应消息签名验证响应
25. 第一响应消息签名验证请求
26. 第一响应消息签名验证响应
27. 与请求相应的处理

图2

加密密钥	权限
客户装置的加密密钥	电子签名的赋予以及验证
数据管理装置的加密密钥	电子签名的验证
数据保管装置的加密密钥	电子签名的验证

图3A

加密密钥	权限
客户装置的加密密钥	电子签名的验证
数据管理装置的加密密钥	电子签名的赋予以及验证
数据保管装置的加密密钥	电子签名的验证

图3B

加密密钥	权限
客户装置的加密密钥	电子签名的验证
数据管理装置的加密密钥	电子签名的验证
数据保管装置的加密密钥	电子签名的赋予以及验证

图3C

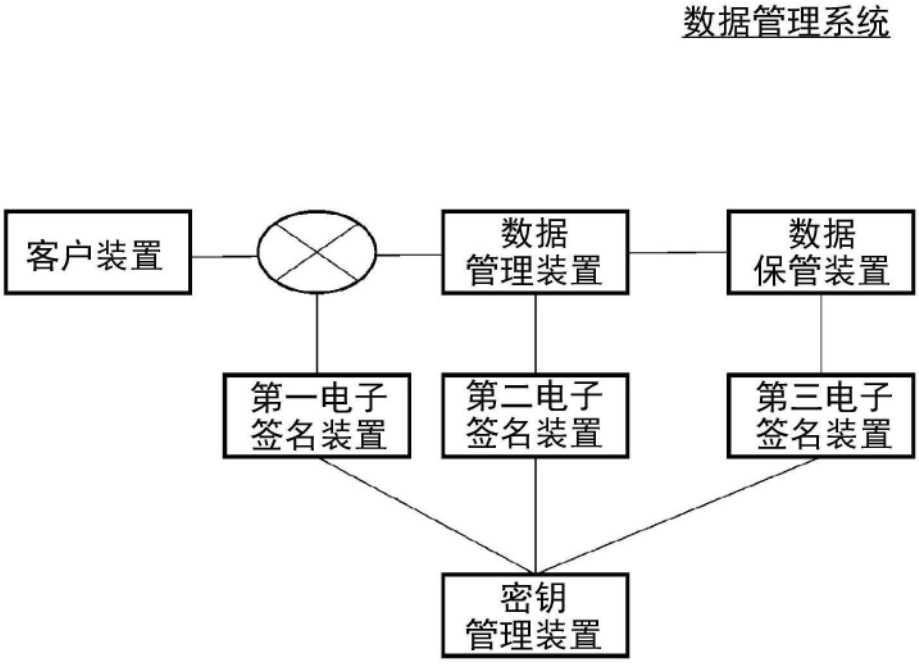
数据管理系统
客户装置
数据
管理装置
数据
保管装置
第一电子
签名装置
第二电子
签名装置
第三电子
签名装置
密钥
管理装置

图4