(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 102144193 B
(45)授权公告日 2013.11.20

(21)申请号 200980134192.2
(22)申请日 2009.09.02
(30)优先权数据
08015433.9 2008.09.02 EP
(85)PCT申请进入国家阶段日
2011.03.02
(86)PCT申请的申请数据
PCT/EP2009/061328 2009.09.02
(87)PCT申请的公布数据
WO2010/026152 DE 2010.03.11
(73)专利权人 西门子公司
地址 德国慕尼黑
(72)发明人 H. 赫尔博特 U. 克雷格
A. 佐比哈德
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 臧永杰 卢江
(51)Int.Cl.
G06F 21/33(2013.01)
G05B 19/406(2006.01)
G05B 19/418(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 1737719 A,2006.02.22, 说明书第12页倒数第2段至第13页倒数第2段、附图5.
US 2006026436 A1,2006.02.02, 说明书第0006段至第0016段, 第0026至第0030段.
WO 2008022606 A1,2008.02.28, 全文.
EP 1696378 A1,2006.08.30, 全文.
EP 1496664 A2,2005.01.12, 全文.
DE 10200681 A1,2003.07.31, 全文.
审查员 王咪娜

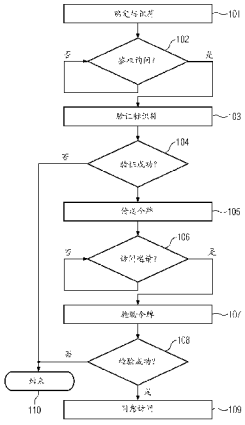
权利要求书2页 说明书4页 附图2页

(54)发明名称

在自动化系统中同意对基于计算机的对象的访问权限的方法、设备和自动化系统

(57)摘要

为了在自动化系统中同意对基于计算机的对象的访问权限，对于控制程序确定标识符，并借助分配给自动化系统的控制和监控单元的私人数字密钥对该标识符加密。根据基于计算机的对象来提供第一业务，和根据控制程序提供自动化系统的第二业务。在向鉴权业务传送时对加密的标识符解密和由鉴权业务验证。鉴权业务在成功的验证时向第二业务传送至少定期有效的令牌。在请求对基于计算机的对象的访问时，通过控制程序向第一业务传送令牌用于检验。在肯定的检验结果时，对于控制程序同意对基于计算机的对象的访问。



CN 102144193 B

1. 用于在自动化系统中同意对基于计算机的对象的访问权限的方法，其中

- 对于控制程序确定标识符，并且借助分配给自动化系统的控制和监控单元的私人数字密钥对标识符加密，

- 根据基于计算机的对象提供第一业务和根据控制程序提供自动化系统的第二业务，

- 在向鉴权业务传送加密的标识符时对加密的标识符解密，并由鉴权业务验证，

- 鉴权业务在成功的验证时向第二业务传送至少定期有效的令牌，

- 在请求对基于计算机的对象的访问时，通过控制程序向第一业务传送令牌用于检验，

- 在肯定的检验结果时，对于控制程序同意对基于计算机的对象的访问。

2. 按照权利要求 1 的方法，其中在面向业务的体系结构之内提供第一业务和第二业务。

3. 按照权利要求 1 或 2 的方法，其中在肯定的检验结果时，由分配给第一业务的授权组件对于控制程序同意对基于计算机的对象的访问。

4. 按照权利要求 1 或 2 的方法，其中加密的标识符和 / 或令牌存储在分配给第二业务的数据库中。

5. 按照权利要求 4 的方法，其中所述数据库包括用于配置第二业务的信息。

6. 按照权利要求 1 或 2 的方法，其中由第二业务请求和由身份管理业务确定控制程序的标识符。

7. 按照权利要求 6 的方法，其中控制和监控单元是用于自动化系统的配置、维护、投入运行和 / 或文件汇编的工程系统，和

其中由所述工程系统提供身份管理业务。

8. 按照权利要求 1 或 2 的方法，其中可以配置第二业务，使得在令牌的有效持续时间结束时第二业务自动地从鉴权业务请求新的令牌。

9. 按照权利要求 1 或 2 的方法，其中在由第二业务所发动的业务调用的范围内向鉴权业务传送加密的标识符。

10. 按照权利要求 1 或 2 的方法，其中在由第二业务所发动的业务调用的范围内向第一业务传送令牌。

11. 按照权利要求 1 或 2 的方法，其中只有在由控制程序将加密的标识符装载到控制程序运行在的计算机单元的工作存储器中时，才对于控制程序同意对基于计算机的对象的访问。

12. 按照权利要求 1 或 2 的方法，其中第二业务对于每一个由第二业务所包括的控制程序模块分别具有特有的业务组件用于请求模块标识符、用于管理由控制和监控单元加密的模块标识符和 / 或用于管理由鉴权业务从模块标识符中所确定的模块令牌。

13. 用于在自动化系统中同意对基于计算机的对象的访问权限的设备，具有

- 用于对于控制程序确定标识符并且借助分配给自动化系统的控制和监控单元的私人数字密钥对标识符加密的装置，

- 用于根据基于计算机的对象提供第一业务和根据控制程序提供自动化系统的第二业务的装置，

- 用于在向鉴权业务传送加密的标识符时对加密的标识符解密并由鉴权业务验证的

装置，

- 用于鉴权业务在成功的验证时向第二业务传送至少定期有效的令牌的装置，

- 用于在请求对基于计算机的对象的访问时通过控制程序向第一业务传送令牌用于检验的装置，

- 用于在肯定的检验结果时对于控制程序同意对基于计算机的对象的访问的装置。

14. 自动化系统，具有

- 在自动化系统的网络节点处的多个经由通信网互相连接的计算机单元，

- 至少一个计算机单元，用于根据基于计算机的对象提供第一业务和根据控制程序提供第二业务，

- 控制和监控单元，用于对于控制程序确定标识符，并且用于借助分配给控制和监控单元的私人数字密钥对标识符加密，

- 分配给鉴权业务的计算机单元，用于对加密的标识符解密和验证并且用于在成功的验证时向第二业务传送至少定期有效的令牌，其中，令牌可被传送给第一业务用于检验并且可被检验用于对于控制程序同意对基于计算机的对象的访问。

在自动化系统中同意对基于计算机的对象的访问权限的方法、设备和自动化系统

技术领域

[0001] 本发明涉及用于在自动化系统中同意对基于计算机的对象的访问权限的方法、计算机程序和自动化系统。

背景技术

[0002] 由于自动化系统的信息技术的不断上升的重要性，用于相对于无权限的访问保护诸如监控、控制和调节设备、传感器和执行元件的联网系统组件的方法增强地获得重要性。与信息技术的另外的应用领域相比，自动化技术中的数据完整性得到特别高的重要性。尤其是在检测、分析和传送测量和控制数据时，可确保存在完整的和未改变的数据。可避免有意的、无意的或由技术故障决定的改变。此外，从具有较多的、但是相对短的报文(Nachricht)的消息通信业务中产生在自动化技术中对于安全技术方法的特别的要求。除此之外，还可考虑自动化系统及其系统组件的实时能力。

[0003] 尤其是在基于面向业务的体系结构的自动化系统中，对于那里所提供的业务可应用常常很不同的安全和访问准则。在此可应用不仅关于用户、而且关于动用另外业务的业务的安全和访问准则。因此在这样的应用领域中软件鉴权获得重大的意义。尤其是在此在大量软件模块的快速和有效的识别和访问授权方面存在要求。迄今的解决方案目的在于软件鉴权方法的明确的实现。这具有以下的缺点，可将相应的鉴权方法固定地集成于要么要求访问要保护的资源、要么提供这些要保护的资源的软件模块中。替代的迄今的解决方案规定，将实现鉴权方法的软件模块静态或动态地与要求或提供要保护的资源的软件模块相捆绑(binden)。如果动态地进行捆绑，则存在至少一种通过配置来控制这点的可能性。

发明内容

[0004] 本发明所基于的任务因此在于，创造一种用于在自动化系统中同意(Einräumung)对基于计算机的对象的访问权限的快速和有效的方法以及说明一种该方法的合适的技术实现。

[0005] 根据本发明通过具有权利要求 1 中所说明的特征的方法、通过具有权利要求 13 中所说明的特征的计算机程序以及通过具有权利要求 14 中所说明的特征的自动化系统来解决该任务。在从属权利要求中说明本发明的有利的改进方案。

[0006] 根据本发明，为了在自动化系统中同意对基于计算机的对象的访问权限，首先对于控制程序确定标识符，并借助分配给自动化系统的控制和监控单元的私人数字密钥对该标识符加密。这可以对于控制程序一次性地进行，并且不需要被重复。优选在面向业务的体系结构之内根据基于计算机的对象来提供第一业务，和根据控制程序提供自动化系统的第二业务。面向业务的或面向服务的体系结构(SOA)目的在于将复杂组识单元中的业务结构化和使之对多个用户可用。在此例如如此来协调数据处理系统的存在的组件、诸如程序、数据库、服务器、或网页，使得将由组件所提供的性能联合成业务和提供给经授权的用户。面

向服务的体系结构能够实现应用集成，其方式是将数据处理系统的各个子组件的复杂性藏匿在标准化接口后面。由此又可以简化访问权限调节。

[0007] 基于计算机的对象例如在不限制该概念的一般性的情况下是操作系统、控制或应用程序，由操作系统、控制或应用程序所提供的业务、性能特征、功能或流程、对外围设备以及位于存储介质上的数据的访问权。功能或流程在此尤其是也包括在自动化系统中访问权限的释放。可将计算机例如理解为 PC、笔记本电脑、服务器、PDA、移动电话以及控制和调节模块、在自动化、车辆、通信或医疗技术中的传感器或执行元件（通常地计算机程序运行于其中的设备）。

[0008] 此外，按照本发明的解决方案，将加密的标识符在向鉴权业务传送时解密，并由鉴权业务验证。鉴权业务在成功的验证时向第二业务传送至少定期有效的令牌。在请求对基于计算机的对象的访问时，通过控制程序向第一业务传送令牌用于检验。在肯定的检验结果时，优选由授权业务对于控制程序同意对基于计算机的对象的访问。可以在由第二业务所发动的业务调用的范围内向鉴权业务传送加密的标识符。以相应的方式可以在由第二业务所发动的业务调用的范围内向第一业务传送令牌。

[0009] 本发明解决方案提供以下的优点，即可以配置要求或提供资源的软件鉴权方法的软件模块，并且不必固定地集成到相应的软件模块中。因此这样的功能性可以以业务组件的形式来使用，并且能够实现快速、灵活和高效的使用。按照本发明的优选的实施形式，第二业务为此对于每一个由第二业务所包括的控制程序模块分别具有特有的业务组件用于请求模块标识符、用于管理由控制和监控单元所加密的模块标识符或用于管理由鉴权业务从模块标识符中所确定的模块令牌。

[0010] 控制和监控单元有利地是用于自动化系统的配置、维护、投入运行和 / 或文件汇编的工程系统，并且由工程系统提供鉴权业务。以此方式可以在基于面向业务的体系结构的分布式自动化系统中特别快速、安全和有效地配置软件鉴权方法。由此产生系统安全性和稳定性的显著的改善。

附图说明

[0011] 以下根据附图借助于实施例详细阐述本发明。

[0012] 图 1 示出用于在自动化系统中同意对基于计算机的对象的访问权限的方法的流程图，

[0013] 图 2 示出用于实现根据图 1 的方法的自动化系统的示意图。

具体实施方式

[0014] 根据图 1 中所表明的用于同意对基于计算机的对象 272 的访问权限的方法，根据图 2 的自动化系统的工程系统 201 对于控制程序 282 确定软件标识符（步骤 101）。此外，借助分配给工程系统 201 的私人数字密钥对软件标识符加密。工程系统 201 经由通信网 205 与第一计算机单元 202、第二计算机单元 203 和第三计算机单元 204 相连接。由第一计算机单元 202 根据基于计算机的对象 272 来提供在面向业务的体系结构之内的第一业务，而根据控制程序 282 来提供第二业务。在第一和第二计算机单元 202、203 的硬盘 223、233 上分别存储有用于实现第一或第二业务的程序代码 207、208。相应的程序代码 207、208 包括基

于计算机的对象 272 或控制程序 282，并且可以装载在第一或第二计算机单元 202、203 的工作存储器 222、232 中。此外，可以由第一或第二计算机单元 202、203 的处理器 221、231 实施相应的程序代码 207、208 用于提供第一或第二业务。

[0015] 在本实施例中，基于计算机的对象 272 是由作为计算机支持的传感器单元的第一计算机单元 202 检测和由在第二计算机单元 203 上运行的控制程序 282 请求的测量结果。控制程序用来操纵第二计算机单元 203 的测量技术方面的或执行元件方面的外围设备，如传感器或机器人。在用于控制和监控计算机单元 202-204 的消息交换方面，可确保使在从发送机到接收机的路径上的消息不失真。否则这可能在自动化系统中导致干扰或损坏。此外，兴趣可能在于，例如只能由经授权的用户询问由于控制程序运行所检测的测量结果，并且不能由未经授权的用户截获和读出具有测量结果的所传送的消息。在此情况下，用户也可以是自动化系统之内的另一个设备。

[0016] 工程系统 201 用于自动化系统的配置、维护、投入运行和 / 或文件汇编 (Dokumentation)，并提供身份管理业务，通过该身份管理业务进行标识符的确定和该标识符的加密。为此在工程系统 201 的硬盘 213 上存储有用于实现身份管理业务的程序代码 206，该程序代码可以被装载到工作存储器 212 中并可由工程系统 201 的处理器 211 实施。鉴权业务包括软件标识符的加密和解密用的业务组件和软件标识符请求的验证用的业务组件。用于实现这些业务组件的程序代码 261、262 同样存储在工程系统 201 的硬盘 213 上。

[0017] 在第三计算机单元 204 的硬盘 243 上存储有用于实现令牌业务的程序代码 209，通过该令牌业务对于控制程序提供用于访问基于计算机的对象的令牌。用于实现令牌业务的程序代码 209 可以被装载到第三计算机单元 204 的工作存储器 242 中，并且可以由第三计算机单元 204 的处理器 241 来实施。

[0018] 由身份管理业务根据具有加密的软件标识符的请求的从第二计算机单元 203 向工程系统 201 所传送的消息 234 来建立根据图 1 中所示出的流程图的步骤 101 确定的和加密的软件标识符。在成功验证询问和建立加密的软件标识符 214 之后，向第二计算机单元 203 传送该软件标识符 214，并在那里存放在分配给第二业务的数据库 283 中，该数据库 283 也包括用于配置第二业务的信息。优选也将软件标识符的未加密的版本向第二计算机单元 203 传送和在那里存储。

[0019] 在建立和向第二计算机单元 203 传送加密的软件标识符之后，令牌业务连续地检验，从第二计算机单元 203 是否存在鉴权询问，该鉴权询问包括具有用于访问基于计算机的对象 272 的第二业务的令牌的请求的消息 235（步骤 102）。具有令牌的请求的消息 235 也包括加密的软件标识符。在向令牌业务传送这种消息时，由令牌业务的相应的业务组件对加密的软件标识符进行解密和验证 (步骤 103)。在此尤其是相对未加密的软件标识符而补偿解密的软件标识符，该未加密的软件标识符优选由具有询问的消息 235 包括。在实际的应用情景中有时较长的时间区间可能处于步骤 102 和步骤 103 之间。

[0020] 紧接着检验，请求和加密的软件标识符的验证是否成功进行 (步骤 104)。在否定的验证结果时，结束本实施例中根据图 1 的方法 (步骤 110)。而如果验证成功进行，则令牌业务促使由令牌业务建立至少定期有效的令牌并向第二业务传送令牌 244（步骤 105）。在那里将令牌存储在分配给第二业务的数据库 283 中。优选如此配置第二业务，使得第二业务

在令牌 244 的有效持续时间结束时自动地从令牌业务请求新的令牌。

[0021] 根据图 1 中所示出的流程图，在步骤 106 中由第一业务连续地检验，是否存在对基于计算机的对象 272 的访问请求。如果存在通过第二业务的具有令牌的访问请求，则第二业务检验令牌的有效性(步骤 108)。紧接着根据步骤 108 询问是否存在成功的检验。在否定的检验结果时，结束图 1 中所表明的方法(步骤 110)。而如果第一业务可以对于令牌 236 执行控制程序 282 的成功的鉴权，则根据步骤 109 对于控制程序 282 由分配给第一业务的授权组件同意对基于计算机的对象 272 的访问。在此在本实施例中，向第二计算机单元 203 传送包括基于计算机的对象 272 的消息(Meldung)224。优选地，只有在由控制程序 282 将加密的软件标识符 214 装载到第二计算机单元 203 的工作存储器 232 中时，才对于控制程序 282 同意对基于计算机的对象 272 的访问。

[0022] 第二业务对于每一个由第二业务所包括的控制程序模块分别具有特有的业务组件用于请求模块标识符、用于管理由控制和监控单元加密的模块标识符和 / 或用于管理由令牌业务从模块标识符中所确定的模块令牌。实现这样的业务组件的程序代码 281 同样存储在第二计算机单元 203 的硬盘 233 上。对于第一业务动用另外业务的应用情况，同样设置第一业务用的相应的业务组件，该业务组件的程序代码 271 存储在第一计算机单元的硬盘 223 上。可能的软件标识符或令牌与用于配置第一业务的数据一起存储在分配给第一计算机单元 202 的数据库 283 中。

[0023] 在工程系统侧，优选通过可以装载到工程系统 202 的工作存储器中的计算机程序来实现上述的方法。计算机程序具有至少一个代码段，在实施该代码段时，对于控制程序确定标识符，并且当计算机程序在计算机中运行时，借助分配给自动化系统的控制和监控单元的私人数字密钥对该标识符加密。在此在面向业务的体系结构之内可以根据基于计算机的对象来提供第一业务，并根据控制程序提供自动化系统的第二业务。此外，在向鉴权业务传送加密的标识符时，由鉴权业务促使该加密的标识符的解密和验证。除此之外，在成功的验证时，由鉴权业务促使向第二业务传送至少定期有效的令牌。在此令牌可以被传送给第一业务用于检验，并且可以被检验用于对于控制程序同意对基于计算机的对象的访问。

[0024] 本发明的应用不局限于所述的实施例。

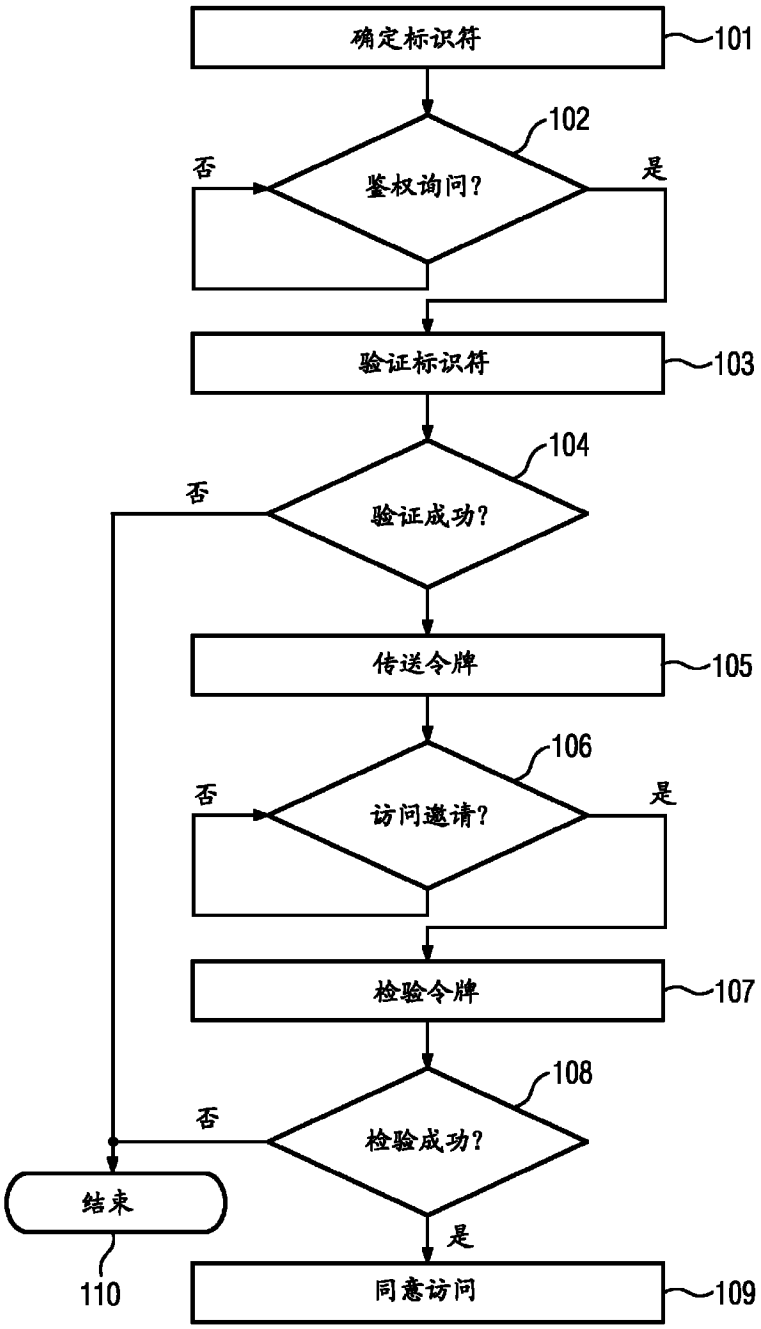

确定标识符
101
102
鉴权询问?
否
是
验证标识符
103
104
验证成功?
否
传送令牌
105
106
访问邀请?
否
是
检验令牌
107
108
检验成功?
否
结束
110
是
同意访问
109

图 1

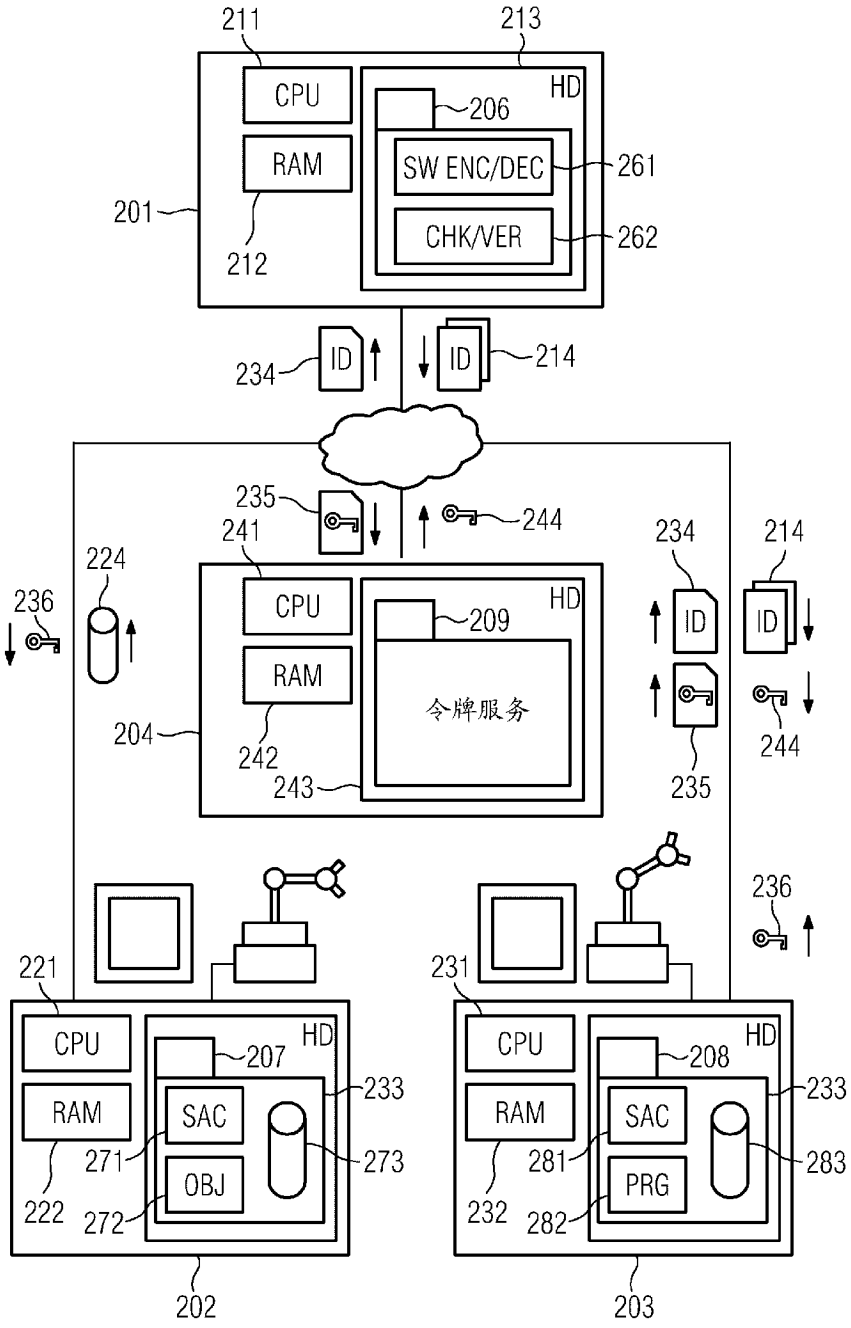

211
213
CPU
HD
206
RAM
SW ENC/DEC
261
201
CHK/VER
262
212
234
ID
ID
214
235
244
241
234
214
224
CPU
HD
236
209
ID
ID
RAM
令牌服务
204
242
244
243
235
236
221
231
CPU
HD
207
CPU
HD
208
233
RAM
SAC
233
271
RAM
SAC
281
273
283
OBJ
PRG
222
272
232
282
202
203

图 2