



(12) 发明专利申请

(10) 申请公布号 CN 102594790 A

(43) 申请公布日 2012. 07. 18

(21) 申请号 201110409320. 9

H04B 5/00 (2006. 01)

(22) 申请日 2011. 12. 01

(30) 优先权数据

2010-273189 2010. 12. 08 JP

(71) 申请人 飞力凯网路股份有限公司

地址 日本东京都

(72) 发明人 关谷秀一 木村光宏 胁直喜

(74) 专利代理机构 北京东方亿思知识产权代理

有限责任公司 11258

代理人 李晓冬

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04W 12/02 (2009. 01)

H04W 12/06 (2009. 01)

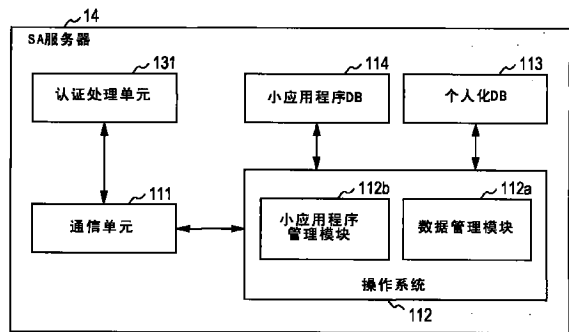
权利要求书 2 页 说明书 17 页 附图 12 页

(54) 发明名称

信息处理设备、信息处理方法、程序和信息系统

(57) 摘要

本发明提供了信息处理设备、信息处理方法、程序和信息系统。信息处理设备与用于执行第一接触式或非接触式通信的电子设备通信并且执行与该电子设备的、不同于第一通信的第二通信。信息处理设备包括：在针对每个电子设备用户的存储区中存储数据的数据存储单元；利用该数据来存储用于与第一通信相关的服务的应用程序的程序存储单元；执行第二通信的通信单元；认证电子设备的认证单元；识别在针对所认证的用户的存储区中所存储的数据的数据识别单元；以及执行单元，该执行单元利用从电子设备发送的并且用于识别用于与第一通信相关的服务的应用程序的识别信息以及所识别的数据，来执行与识别信息相对应的应用程序。



1. 一种用于与电子设备通信的信息处理设备,所述电子设备执行接触式或非接触式的第一通信,所述信息处理设备执行与所述电子设备的第二通信,第二通信不同于第一通信,所述信息处理设备包括:

数据存储单元,所述数据存储单元被配置为在针对使用所述电子设备的每个用户的存储区中存储数据项;

程序存储单元,所述程序存储单元被配置为利用所述数据项来存储执行与第一通信相关的服务的应用程序;

通信单元,所述通信单元被配置为执行与所述电子设备的第二通信;

认证单元,所述认证单元被配置为认证所述电子设备;

数据识别单元,所述数据识别单元被配置为基于从所述认证单元认证的所述电子设备发送的认证信息,来识别在所述数据存储单元的针对所述认证单元认证的所述电子设备的用户的存储区中所存储的数据项;以及

执行单元,所述执行单元被配置为基于从所述电子设备发送的并且用于识别执行与第一通信相关的服务的所述应用程序的识别信息以及由所述数据识别单元识别的数据项,来执行与所述识别信息相对应的所述应用程序。

2. 根据权利要求1所述的信息处理设备,其中所述数据识别单元响应于从提供内容给所述电子设备的并且被所述电子设备认证的提供设备经由所述电子设备发送的请求,来识别在针对所述电子设备的用户的存储区中所存储的数据项。

3. 根据权利要求1所述的信息处理设备,其中所述数据识别单元响应于从提供内容给所述电子设备的并且被所述电子设备认证的提供设备直接发送的请求,来识别在针对所述电子设备的用户的存储区中所存储的数据项。

4. 根据权利要求1所述的信息处理设备,其中所述认证单元认证提供内容给所述电子设备的提供设备,并且其中所述数据识别单元响应于从被所述认证单元认证的所述提供设备发送的请求,来识别在针对所述电子设备的用户的存储区中所存储的数据项。

5. 根据权利要求1所述的信息处理设备,其中所述通信单元向所述电子设备发送在所述数据存储单元的针对所述认证单元认证的所述电子设备的用户的存储区中所存储的数据项的副本,并且其中响应于作为所述电子设备中对用于执行与第一通信相关的服务的所述应用程序的仿真的结果而从所述电子设备执行的第一通信的通信伙伴发送的请求,所述数据识别单元识别所述数据项。

6. 一种用在信息处理设备中的信息处理方法,所述信息处理设备用于与电子设备通信,所述电子设备执行接触式或非接触式的第一通信,所述信息处理设备执行与所述电子设备的第二通信,第二通信不同于第一通信,所述信息处理设备包括:数据存储单元,所述数据存储单元被配置为在针对使用所述电子设备的每个用户的存储区中存储数据项;程序存储单元,所述程序存储单元被配置为利用所述数据项来存储执行与第一通信相关的服务的应用程序;以及通信单元,所述通信单元被配置为执行与所述电子设备的第二通信,所述方法包括:

认证所述电子设备;

基于从所认证的电子设备发送的认证信息来识别在所述数据存储单元的针对所认证的电子设备的用户的存储区中所存储的数据项;以及

基于从所述电子设备发送的并且用于识别执行与第一通信相关的服务的所述应用程序的识别信息以及所识别的数据项,来执行与所述识别信息相对应的所述应用程序。

7. 一种程序,包括:

用于使计算机执行信息处理设备中所执行的处理的程序代码,所述信息处理设备用于与电子设备通信,所述电子设备执行接触式或非接触式的第一通信,所述信息处理设备执行与所述电子设备的第二通信,第二通信不同于第一通信,所述信息处理设备包括:数据存储单元,所述数据存储单元被配置为在针对使用所述电子设备的每个用户的存储区中存储数据项;程序存储单元,所述程序存储单元被配置为利用所述数据项来存储执行与第一通信相关的服务的应用程序;以及通信单元,所述通信单元被配置为执行与所述电子设备的第二通信,所述处理包括:认证所述电子设备;基于从所认证的电子设备发送的认证信息来识别在所述数据存储单元的针对所认证的电子设备的用户的存储区中所存储的数据项;以及基于从所述电子设备发送的并且用于识别执行与第一通信相关的服务的所述应用程序的识别信息以及所识别的数据项,来执行与所述识别信息相对应的所述应用程序。

8. 一种信息处理系统,包括:

电子设备,所述电子设备执行接触式或非接触式的第一通信;以及

第一信息处理设备和第二信息处理设备,第一信息处理设备和第二信息处理设备用于与所述电子设备通信,第一信息处理设备和第二信息处理设备执行与所述电子设备的、不同于第一通信的第二通信;

其中第一信息处理设备包括:认证单元,所述认证单元被配置为认证所述电子设备,并且其中第二信息处理设备包括:数据存储单元,所述数据存储单元被配置为在针对使用所述电子设备的每个用户的存储区中存储数据项,程序存储单元,所述程序存储单元被配置为利用所述数据项来存储执行与第一通信相关的服务的应用程序,通信单元,所述通信单元被配置为执行与所述电子设备的第二通信,认证单元,所述认证单元被配置为认证所述电子设备,数据识别单元,所述数据识别单元被配置为基于从第一信息处理设备认证的所述电子设备发送的认证信息来识别在所述数据存储单元的针对第一信息处理设备认证的所述电子设备的用户的存储区中所存储的数据项,以及执行单元,所述执行单元被配置为基于从所述电子设备发送的并且用于识别执行与第一通信相关的服务的所述应用程序的识别信息以及由所述数据识别单元识别的数据项,来执行与所述识别信息相对应的所述应用程序。

信息处理设备、信息处理方法、程序和信息处理系统

技术领域

[0001] 本公开涉及信息处理设备、信息处理方法、程序和信息处理系统，并且具体地涉及能够以安全的方式跨越终端设备的所有平台来提供服务的信息处理设备、信息处理方法、程序和信息处理系统。

背景技术

[0002] 近些年中，包括了执行接触式或非接触式近场通信的集成电路（IC）芯片的移动终端设备（例如，蜂窝电话）已通过执行与短程通信相关的应用程序来提供各种服务。

[0003] 然而，因为用于存储应用程序的移动终端设备的存储器的容量是有限的，所以可提供的服务的数目是有限的。

[0004] 为了应对这样的问题，已开发了如下的系统：在该系统中，与短程通信相关的应用程序被存储在服务器中的具有特有（unique）识别信息项的存储区中，并且当移动终端设备启动服务时，与该服务相对应的应用程序被在服务器上执行（例如参见日本未经实审专利申请公布 No. 2002-354143）。这样的系统使移动终端设备能在不管移动终端设备的存储器的容量如何的情况下提供服务。

发明内容

[0005] 然而，日本未经实审专利申请公布 No. 2002-354143 没有描述通过应用程序在服务器上的执行而被处理的数据。

[0006] 例如，日本未经实审专利申请公布 No. 2002-354143 没有描述通过应用程序在服务器上的执行而被处理的数据是否被存储在服务器中。因此，如果通过应用程序的执行而处理的数据被存储在移动终端设备中，则数据的量被移动终端设备的存储器的容量所限制。

[0007] 此外，日本未经实审专利申请公布 No. 2002-354143 没有描述通过应用程序在服务器上的执行而被处理的数据的安全性如何被确保。

[0008] 因此，本公开提供能够以安全方式跨越终端设备的所有平台来提供服务的信息处理设备、信息处理方法、程序和信息处理系统。

[0009] 根据本公开的一个实施例，提供了一种用于与执行第一接触式或非接触式通信的电子设备通信的信息处理设备。该信息处理设备执行与电子设备的、不同于第一通信的第二通信。该信息处理设备包括：数据存储单元，该数据存储单元被配置为在针对使用电子设备的每个用户的存储区中存储数据项；程序存储单元，该程序存储单元被配置为利用数据项来存储执行与第一通信相关的服务的应用程序；通信单元，该通信单元被配置为执行第二通信；认证单元，该认证单元被配置为认证电子设备；数据识别单元，该数据识别单元被配置为识别在针对认证单元认证的电子设备的用户的存储区中所存储的数据项；以及执行单元，该执行单元被配置为基于从电子设备发送的并且用于识别执行与第一通信相关的服务的应用程序的识别信息以及由数据识别单元识别的数据项，来执行与识别信息相对应的

应用程序。

[0010] 数据识别单元可以响应于从提供内容给电子设备的并且被电子设备认证的提供设备经由电子设备发送的请求,来识别在针对电子设备的用户的存储区中所存储的数据项。

[0011] 数据识别单元可以响应于从提供内容给电子设备的并且被电子设备认证的提供设备直接发送的请求,来识别在针对电子设备的用户的存储区中所存储的数据项。

[0012] 认证单元可以认证提供内容给电子设备的提供设备,并且数据识别单元可以响应于从被认证单元认证的提供设备发送的请求,来识别在针对电子设备的用户的存储区中所存储的数据项。

[0013] 通信单元可以向电子设备发送在数据存储单元的针对认证单元认证的电子设备的用户的存储区中所存储的数据项的副本,并且响应于作为电子设备中用于执行与第一通信相关的服务的应用程序的仿真的结果而从电子设备执行的第一通信的通信伙伴发送的请求,数据识别单元可以识别数据项。

[0014] 根据本公开的另一个实施例,提供了一种用在信息处理设备中的信息处理方法,该信息处理设备用于与执行第一接触式或非接触式通信的电子设备通信。信息处理设备执行与电子设备的、不同于第一通信的第二通信。信息处理设备包括:数据存储单元,该数据存储单元被配置为在针对使用电子设备的每个用户的存储区中存储数据项;程序存储单元,该程序存储单元被配置为利用数据项来存储执行与第一通信相关的服务的应用程序;以及通信单元,该通信单元被配置为执行第二通信。所述方法包括:认证电子设备;基于从所认证的电子设备发送的认证信息来识别在数据存储单元的针对所认证的电子设备的用户的存储区中所存储的数据项;以及基于从电子设备发送的并且用于识别执行与第一通信相关的服务的应用程序的识别信息以及所识别的数据项,来执行与识别信息相对应的应用程序。

[0015] 根据本公开的又一个实施例,一种程序包括用于使计算机执行信息处理设备中所执行的处理的程序代码,该信息处理设备用于与执行第一接触式或非接触式通信的电子设备通信,其中信息处理设备执行与电子设备的、不同于第一通信的第二通信。信息处理设备包括:数据存储单元,该数据存储单元被配置为在针对使用电子设备的每个用户的存储区中存储数据项;程序存储单元,该程序存储单元被配置为利用数据项来存储执行与第一通信相关的服务的应用程序;以及通信单元,该通信单元被配置为执行第二通信。所述处理包括:认证电子设备;基于从所认证的电子设备发送的认证信息来识别在数据存储单元的针对所认证的电子设备的用户的存储区中所存储的数据项;以及基于从电子设备发送的并且用于识别执行与第一通信相关的服务的应用程序的识别信息以及所识别的数据项,来执行与识别信息相对应的应用程序。

[0016] 根据本公开的再一个实施例,一种信息处理系统包括:电子设备,该电子设备执行第一接触式或非接触式通信;以及第一信息处理设备和第二信息处理设备,该第一信息处理设备和该第二信息处理设备用于与电子设备通信,其中第一信息处理设备和第二信息处理设备执行与电子设备的、不同于第一通信的第二通信。第一信息处理设备包括:认证单元,该认证单元被配置为认证电子设备,并且第二信息处理设备包括:数据存储单元,该数据存储单元被配置为在针对使用电子设备的每个用户的存储区中存储数据项,程序存储单

元,该程序存储单元被配置为利用数据项来存储执行与第一通信相关的服务的应用程序,通信单元,该通信单元被配置为执行第二通信,认证单元,该认证单元认证电子设备,数据识别单元,该数据识别单元被配置为基于从第一信息处理设备认证的电子设备发送的认证信息来识别在数据存储单元的针对第一信息处理设备认证的电子设备的用户的存储区中所存储的数据项,以及执行单元,该执行单元被配置为基于从电子设备发送的并且用于识别执行与第一通信相关的服务的应用程序的识别信息以及由数据识别单元识别的数据项,来执行与识别信息相对应的应用程序。

[0017] 根据本公开的实施例,电子设备被认证,被存储在针对认证单元认证的电子设备的用户的存储区中的数据项被识别,并且基于从电子设备发送的并且用于识别执行与第一通信相关的服务的应用程序的识别信息以及由数据识别单元识别的数据项,与识别信息相对应的应用程序被执行。

[0018] 根据本公开的实施例,可以以安全的方式跨越终端设备的所有平台来提供服务。

附图说明

- [0019] 图 1 是根据本公开的实施例的信息处理系统的示例性配置的框图;
- [0020] 图 2 是移动终端设备的示例性配置的框图;
- [0021] 图 3 是认证服务器的示例性配置的框图;
- [0022] 图 4 是移动终端设备的示例性功能配置的框图;
- [0023] 图 5 是认证服务器的示例性功能配置的框图;
- [0024] 图 6 是 SA 服务器的示例性功能配置的框图;
- [0025] 图 7 是示出服务提供处理的示例的流程图;
- [0026] 图 8 是 SA 服务器的另一示例性功能配置的框图;
- [0027] 图 9 是其中用户数据被参考或更新的信息处理系统的示例性配置的框图;
- [0028] 图 10 是示出用于参考或更新用户数据的处理的示例的流程图;
- [0029] 图 11 是示出用于参考或更新用户数据的处理的另一示例的流程图;
- [0030] 图 12 是示出用于参考或更新用户数据的处理的又一示例的流程图;
- [0031] 图 13 是提供高速服务的信息处理系统的示例性配置的框图;并且
- [0032] 图 14 是示出高速服务提供处理的示例的流程图。

具体实施方式

[0033] 下面参考附图来描述本公开的示例性实施例。

[0034] < 信息处理系统的示例性配置 >

[0035] 图 1 是根据本公开的实施例的信息处理系统的示例性配置的框图。如图 1 所示,信息处理系统向使用移动终端设备 11 的用户提供服务,例如电子货币服务、检票服务、考勤服务或门禁管理服务。

[0036] 移动终端设备 11 被配置为移动电子设备,例如蜂窝电话或个人数字助理 (PDA)。移动终端设备 11 执行与读出器 / 写入器 12 的近场通信 (NFC)。当彼此通信的设备之间的距离小于几十厘米时,近场通信被启动。近场通信是设备之间的非接触式通信。读出器 / 写入器 12 与服务器 (未示出) 连接。读出器 / 写入器 12 执行与移动终端设备 11 的近场

通信,并且此后向服务器供应通过通信获取的信息。

[0037] 此外,移动终端设备 11 执行与基站(未示出)的无线通信。因此,移动终端设备 11 经由与基站连接的诸如因特网之类的网络与认证服务器 13 和安全应用(SA)服务器 14 通信。认证服务器 13 和 SA 服务器 14 经由诸如因特网之类的网络彼此相连接。认证服务器 13 与移动终端设备 11 通信并且执行对移动终端设备 11 的认证处理。SA 服务器 14 与移动终端设备 11 通信并且执行用于向使用移动终端设备 11 的用户提供服务的程序。以此方式,服务可被提供给用户。此外,移动终端设备 11、认证服务器 13 和 SA 服务器 14 是防篡改的(tamper resistant)。在移动终端设备 11 与认证服务器 13 之间并且在移动终端设备 11 与 SA 服务器 14 之间执行相互认证。

[0038] <移动终端设备的示例性配置>

[0039] 接下来参考图 2 来描述移动终端设备 11 的示例性配置。

[0040] 在图 2 中,中央处理单元(CPU)31 根据只读存储器(ROM)32 中存储的程序或者加载到随机存取存储器(RAM)33 中的程序来执行各种处理。RAM 33 还存储 CPU 31 执行各种处理所必要的的数据。

[0041] CPU 31、ROM 32 和 RAM 33 经由总线 34 彼此连接。总线 34 还有着输入/输出接口 35 与它连接。

[0042] 输入/输出接口 35 有着以下单元与它连接:包括键、按钮、触摸板和麦克风的输入单元 36,从例如 LCD(液晶显示器)或有机电致发光(EL)显示器形成的显示器,从例如扬声器形成的输出单元 37,从例如硬盘形成的存储单元 38,从例如用于无线通信的天线形成的第一通信单元 39,以及从例如用于近场通信的天线形成的第二通信单元 40。

[0043] 存储单元 38 例如存储用于认证移动终端设备 11 的并且移动终端设备 11 所特有的信息。

[0044] 第一通信单元 39 执行与基站(未示出)的无线通信处理。第二通信单元 40 执行与读出器/写入器 12 的近场通信处理。

[0045] 当必要时,输入/输出接口 35 还有着驱动器 41 与它连接。当必要时,从例如半导体存储器形成的可移除介质 42 被安装在驱动器 41 中。当必要时,由可移除介质 42 读出的计算机程序被安装在存储单元 38 中。

[0046] <认证服务器的示例性配置>

[0047] 接下来参考图 3 来描述认证服务器 13 的示例性配置。

[0048] 如图 3 所示,CPU 51 根据 ROM 52 中存储的程序或者 RAM 53 中存储的程序来执行各种处理。RAM 53 还存储 CPU 51 执行各种处理所必要的的数据。

[0049] CPU 51、ROM 52 和 RAM 53 经由总线 54 彼此连接。总线 54 还有着输入/输出接口 55 与它连接。

[0050] 输入/输出接口 55 有着以下单元与它连接:包括键盘和鼠标的输入单元 56,从例如阴极射线管(CRT)或液晶显示器(LCD)形成的显示器,从例如扬声器形成的输出单元 57,从例如硬盘形成的存储单元 58,以及从例如调制解调器或终端适配器形成的通信单元 59。

[0051] 通信单元 59 经由诸如因特网之类的网络执行通信处理。

[0052] 当必要时,输入/输出接口 55 还有着驱动器 60 与它连接。当必要时,从例如磁盘、光盘、磁光盘或半导体存储器形成的可移除介质 61 被安装在驱动器 60 中。当必要时,由可

移除介质 61 读出的计算机程序被安装在存储单元 58 中。

[0053] 注意,因为 SA 服务器 14 的配置类似于图 3 所示的认证服务器 13 的配置,所以对其的描述未被重复。

[0054] < 移动终端设备的示例性功能配置 >

[0055] 接下来参考图 4 来描述移动终端设备 11 的示例性功能配置。

[0056] 如图 4 所示,移动终端设备 11 包括设备驱动器 71、虚拟机 72、中间件 73、VSE 小应用程序 (applet)74、通信单元 75、安全元件 (secureelement)76 和无接触式前端 (contactless front-end) (CLF)77。注意,在图 4 所示的移动终端设备 11 中,被虚线包围的设备驱动器 71、虚拟机 72、中间件 73 和虚拟安全元件 (VSE) 小应用程序 74 由 CPU 31 来实现 (参见图 2)。此外,上下关系表示了层。

[0057] 设备驱动器 71 控制设备,例如通信单元 75、安全元件 76 和 CLF77。

[0058] 虚拟机 72 例如被配置为诸如 Dalvik 虚拟机之类的处理虚拟机。

[0059] 中间件 73 具有应用程序接口 (API) 并且向 VSE 小应用程序 74 提供与预定通信相关的功能。例如,中间件 73 向 VSE 小应用程序 74 提供访问安全元件 76 的功能以及经由通信单元 75 和 CLF 77 进行通信的功能。注意,部分的或全部的中间件 73 可位于设备驱动器 71 与虚拟机 72 之间的层中。

[0060] 例如,VSE 小应用程序 74 是在虚拟机 72 上运行的应用程序。当移动终端设备 11 被用户操作时,VSE 小应用程序 74 执行与操作相对应的处理。更具体地,VSE 小应用程序 74 根据移动终端设备 11 的认证的结果来执行与读出器 / 写入器 12 和 SA 服务器 14 之间的通信相关的处理。

[0061] 通信单元 75 对应于图 2 所示的第一通信单元 39。通信单元 75 与基站 (未示出) 通信并且此后与认证服务器 13 和 SA 服务器 14 通信。

[0062] 当与和读出器 / 写入器 12 的近场通信相关的应用程序被执行时,安全元件 76 存储安全数据。作为移动终端设备 11 特有的信息的安全 ID 被分配给安全元件 76。在现有技术中,安全元件存储起到被执行用于提供服务 (例如,电子货币服务) 的应用程序的作用的小应用程序、以及持久的 (persisted) 用户数据 (在下面描述)。对比地,在根据本实施例的信息处理系统中,小应用程序和用户数据被存储在 SA 服务器 14 中。

[0063] CLF 77 对应于图 2 所示的第二通信单元 40。CLF 77 包括用于执行与读出器 / 写入器 12 的近场通信的天线以及用于控制近场通信的控制器。CLF 77 执行与读出器 / 写入器 12 的近场通信。

[0064] < 认证服务器的示例性功能配置 >

[0065] 接下来参考图 5 来描述认证服务器 13 的示例性功能配置。

[0066] 如图 5 所示,认证服务器 13 包括通信单元 91 和认证处理单元 92。

[0067] 通信单元 91 对应于图 3 所示的通信单元 59。通信单元 91 经由诸如因特网之类的网络与移动终端设备 11 和 SA 服务器 14 通信。

[0068] 基于经由通信单元 91 从移动终端设备 11 发送的并且用于认证移动终端设备 11 的认证信息 (例如,安全 ID),认证处理单元 92 认证移动终端设备 11。如果移动终端设备 11 被成功认证,则认证处理单元 92 经由通信单元 91 向移动终端设备 11 供应用于访问 SA 服务器 14 的访问信息。

[0069] <SA 服务器的示例性功能配置>

[0070] 接下来参考图 6 来描述 SA 服务器 14 的示例性功能配置。

[0071] 如图 6 所示, SA 服务器 14 包括通信单元 111、操作系统 112、小应用程序数据库 (DB) 114 和个人化 DB 113。

[0072] 通信单元 111 经由诸如因特网之类的网络 (未示出) 与移动终端设备 11 和认证服务器 13 通信。

[0073] 操作系统 112 执行 SA 服务器 14 的总体控制和管理。操作系统 112 包括数据管理模块 112a 和小应用程序管理模块 112b。

[0074] 数据管理模块 112a 起到了文件系统的作用。数据管理模块 112a 管理个人化 DB 113 中存储的数据项 (在下文中被称为“用户数据项”)。通过使用经由通信单元 111 从移动终端设备 11 发送的、移动终端设备 11 的认证信息 (安全 ID), 数据管理模块 112a 从个人化 DB 113 中存储的用户数据项之中识别与认证信息相关联的用户数据项。

[0075] 小应用程序管理模块 112b 管理小应用程序 DB 114 中存储的小应用程序 (应用程序)。通过使用经由通信单元 111 从移动终端设备 11 供应的并且用于识别小应用程序的识别信息, 小应用程序管理模块 112b 从小应用程序 DB 114 中存储的小应用程序之中选择与识别信息相对应的小应用程序。此后, 小应用程序管理模块 112b 启动 (执行) 与识别信息相对应的小应用程序。

[0076] 个人化 DB 113 具有针对移动终端设备 11 (即用户) 特有的认证信息项中的每一个的存储区。个人化 DB 113 在每个存储区中存储与认证信息项之一相对应的用户数据项。在个人化 DB 113 中, 针对用户的存储区中的每一个中存储的用户数据是持久的数据。

[0077] 小应用程序 DB 114 存储要被执行用于向移动终端设备 11 的用户提供服务 (例如, 电子货币服务) 的小应用程序。小应用程序 DB 114 中存储的每个小应用程序都具有小应用程序特有的被分配的识别信息。当小应用程序特有的识别信息被从移动终端设备 11 发送时, 小应用程序 DB 114 中存储的小应用程序被启动。注意, 在小应用程序 DB 114 中, 针对提供小应用程序的内容提供者中的每一个来预先登录小应用程序。

[0078] 小应用程序 DB 114 存储例如具有 **FeliCa®** OS 功能的小应用程序。一般地, FeliCa OS 执行与诸如电子货币服务之类的服务相关的处理。包括 FeliCa OS 的电子设备代替信用卡或预付卡而被用于商业交易。在 SA 服务器 14 中, 操作系统 112 的小应用程序管理模块 112b 启动原来安装在移动终端设备 11 中的、诸如 FeliCa OS 之类的接触式或非接触式 IC 卡小应用程序。以此方式, SA 服务器 14 通过与移动终端设备 11 的通信向移动终端设备 11 的用户提供诸如电子货币服务之类的服务。

[0079] 如上所述, 可以在 SA 服务器 14 上启动原来在移动终端设备 11 上运行的并且执行与和读出器 / 写入器 12 的近场通信相关的服务的小应用程序。

[0080] <用户登录>

[0081] 接下来描述由移动终端设备 11 执行的用户登录。

[0082] 首先, 为了申请对某内容提供者所提供的小应用程序的使用的登录, 用户在移动终端设备 11 上执行操作。移动终端设备 11 显示 Web 浏览器的用户登录画面。在此时, VSE 小应用程序 74 被启动。VSE 小应用程序 74 将移动终端设备 11 连接到认证服务器 13。此后, 认证服务器 13 的认证处理单元 92 通过经由 VSE 小应用程序 74 认证安全元件 76, 来认

证移动终端设备 11。如果移动终端设备 11 被成功地认证,则认证服务器 13 通过 VSE 小应用程序 74 获取安全元件 76 中存储的安全 ID。更具体地,VSE 小应用程序 74 访问安全元件 76 并且获取安全 ID。随后,VSE 小应用程序 74 经由通信单元 75 向认证服务器 13 发送(供应)所获取的安全 ID。安全 ID 用作了关于移动终端设备 11 的认证信息。

[0083] 认证服务器 13 向 SA 服务器 14 发送(供应)所获取的安全 ID。在 SA 服务器 14 中,操作系统 112 在存储单元(未示出)中存储从认证服务器 13 接收的安全 ID。以此方式,用户登录被完成。注意,在同时,对内容提供者而言必要的、诸如会员号和名字之类的关于用户的个人信息(个人化数据)也与安全 ID 一起被存储。此外,在 SA 服务器 14 中,数据管理模块 112a 获取个人化 DB 113 中的与安全 ID 相对应的存储区,在该存储区中生成要由已被用户登录的小应用程序使用的数据区,并且将数据(用户数据)设置为初始值。

[0084] 虽然已参考通过 VSE 小应用程序 74 执行的登录来描述了用户登录,但是用户登录不限于此。例如,可以根据用户在 Web 浏览器中显示的用户登录画面上执行的操作、通过内容提供者(CP)所拥有的内容提供者(CP)服务器来进行用户登录。

[0085] < 服务提供处理的示例 >

[0086] 接下来参考图 7 所示的流程图来描述当以上述方式启动 SA 服务器 14 中存储的小应用程序时所执行的服务提供处理的示例。

[0087] 在此情况下,为了接收所希望的服务,用户将他们的移动终端设备 11 移动得较接近读出器/写入器 12,以使得移动终端设备 11 执行与读出器/写入器 12 的近场通信。

[0088] 例如,如果用户轻敲移动终端设备 11 的显示画面上显示的 VSE 小应用程序 74 的图标,则在步骤 S11 中,移动终端设备 11 启动 VSE 小应用程序 74。VSE 小应用程序 74 将移动终端设备 11 连接到认证服务器 13(步骤 S12 和 S31)。在步骤 S32 中,认证服务器 13 的认证处理单元 92 经由 VSE 小应用程序 74 认证安全元件 76 并且因此认证移动终端设备 11。如果移动终端设备 11 被成功地认证,则 VSE 小应用程序 74 访问安全元件 76 并且获取安全 ID。

[0089] 在步骤 S13 中,VSE 小应用程序 74 经由通信单元 75、基站和诸如因特网之类的网络向认证服务器 13 发送(供应)所获取的安全 ID。

[0090] 在步骤 S33 中,认证服务器 13 的通信单元 91 接收经由诸如因特网之类的网络从移动终端设备 11 发送的安全 ID,并且将安全 ID 供应给认证处理单元 92。

[0091] 在步骤 S33 中安全 ID 被从通信单元 91 供应给认证处理单元 92 之后,认证处理单元 92 发出一次性的(one-time)统一资源定位符(URL)。一次性 URL 被用于移动终端设备 11 访问 SA 服务器 14 并且仅有效一次。注意,用于移动终端设备 11 访问 SA 服务器 14 的访问信息不限于一次性 URL。其他信息可被使用。

[0092] 在步骤 S34 中,认证服务器 13 的通信单元 91 经由诸如因特网之类的网络和基站向 VSE 小应用程序 74 发送由认证处理单元 92 发出的一次性 URL。

[0093] 一在步骤 S14 中接收到来自认证服务器 13 的一次性 URL,VSE 小应用程序 74 就在步骤 S15 中基于一性 URL 向 SA 服务器 14 发送连接请求。注意,连接请求包括安全 ID。

[0094] 在步骤 S51 中,SA 服务器 14 的通信单元 111 从 VSE 小应用程序 74 接收连接请求。操作系统 112 基于从 VSE 小应用程序 74 接收的连接请求中所包括的安全 ID 来验证连接请求是从登录用户发送的。在步骤 S52 中,通信单元 111 向 VSE 小应用程序 74 发送对连接请

求的响应。在步骤 S16 中,VSE 小应用程序 74 从 SA 服务器 14 接收响应。以此方式,VSE 小应用程序 74(移动终端设备 11)与 SA 服务器 14 之间的连接被建立。

[0095] 随后,在步骤 S53 中,SA 服务器 14 的操作系统 112 进入待机模式,直到小应用程序被启动。

[0096] 此外,在步骤 S17 中,VSE 小应用程序 74 激活移动终端设备 11。更具体地,VSE 小应用程序 74 改变移动终端设备 11 的显示画面的显示颜色并且使 CLF 77 进入近场通信的待机模式。

[0097] 在此时,因为移动终端设备 11 的显示画面的显示颜色被改变,所以用户辨认出移动终端设备 11 可执行近场通信并且将移动终端设备 11 移到读出器 / 写入器 12 上(将移动终端设备 11 移动得较接近读出器 / 写入器 12)。

[0098] 当移动终端设备 11 和读出器 / 写入器 12 彼此接近时,在步骤 S71 中,读出器 / 写入器 12 发送轮询命令(在下文中简称为“轮询”)给 CLF 77。一在步骤 S91 中接收到来自读出器 / 写入器 12 的轮询,CLF 77 就在步骤 S92 中向读出器 / 写入器 12 发送对轮询的响应。在步骤 S72 中,读出器 / 写入器 12 从 CLF 77 接收响应。以此方式,通过发送轮询,读出器 / 写入器 12 将移动终端设备 11 辨认为通信伙伴。

[0099] 在此情况下,移动终端设备 11 与读出器 / 写入器 12 之间执行的近场通信的通信协议是由 ISO 14443 定义的 Type A 或 Type B。这样的协议(通信方法)中所用的通用命令格式之一是由 ISO 7816-4 定义的被称为应用协议数据单元(APDU)的命令格式。在下文中,符合 APDU 命令格式的命令被称为“APDU 命令”。

[0100] 往回参考图 7,在步骤 S71、S72、S91 和 S92 中的处理已被完成之后,利用 Type A 或 Type B 方法的通信被在移动终端设备 11 与读出器 / 写入器 12 之间重复。以此方式,基于 ISO 14443-3 的通信被执行。在步骤 S73 中,为了选择小应用程序(应用)中的一个并且启动小应用程序,读出器 / 写入器 12 发送 APDU 命令“选择(AID)”给 CLF 77。

[0101] 注意,AID(应用标识符)是由 ISO 7816-5 定义的识别信息。AID 用于识别小应用程序。AID 被唯一地分配给小应用程序。

[0102] 在步骤 S93 中,一接收到来自读出器 / 写入器 12 的选择(AID),CLF77 就将所接收的选择(AID)供应给 VSE 小应用程序 74。

[0103] 一在步骤 S18 中接收到来自 CLF 77 的选择(AID),VSE 小应用程序 74 就将所接收的选择(AID)供应给 SA 服务器 14。

[0104] 注意,例如,超文本传输协议(HTTP)或者具有高于 HTTP 的安全等级的安全等级的安全超文本传输协议(HTTPS)被用作 VSE 小应用程序 74(移动终端设备 11)与 SA 服务器 14 之间执行的通信的通信协议。更具体地,例如,瘦客户端应用协议(TCAP)被使用。TCAP 是用于符合 FeLiCa 的服务器应用经由网络操纵符合 FeLiCa 的蜂窝电话或读出器 / 写入器的协议。TCAP 用于例如电子支付。然而,移动终端设备 11 与 SA 服务器 14 之间的通信协议不限于 HTTP 或 HTTPS。例如,TCP/IP(传输控制协议 / 因特网协议)可被用作通信协议。

[0105] 在步骤 S54 中,SA 服务器 14 的通信单元 111 从 VSE 小应用程序 74 接收选择(AID)并且将所接收的选择(AID)供应给操作系统 112。

[0106] 在步骤 S55 中,操作系统 112 的数据管理模块 112a 基于步骤 S51 中接收的安全 ID 和从 VSE 小应用程序 74 接收的选择(AID)而从与安全 ID 相对应的个人化 DB 113 的存储

区中的用户数据项之中识别用于通过选择 (AID) 中的 AID 所识别的小应用程序的数据区中的用户数据项。

[0107] 在步骤 S56 中,操作系统 112 的小应用程序管理模块 112b 利用由数据管理模块 112a 识别的用户数据项而从小应用程序 DB 114 中选择与从 VSE 小应用程序 74 接收的选择 (AID) 中的 AID 相对应的小应用程序,并且启动所选择的小应用程序。

[0108] 在步骤 S57 中,操作系统 112 将对选择 (AID) 的响应供应给通信单元 111 并且使通信单元 111 利用 TCAP 向 VSE 小应用程序 74 发送响应。

[0109] 在步骤 S19 中,一接收到来自 SA 服务器 14 的对选择 (AID) 的响应,VSE 小应用程序 74 就向 CLF 77 发送对所接收的选择 (AID) 的响应。

[0110] 在步骤 S94 中,一接收到来自 VSE 小应用程序 74 的响应,CLF 77 就向读出器 / 写入器 12 发送所接收的响应。在步骤 S74 中,读出器 / 写入器 12 从 CLF 77 接收响应。

[0111] 在步骤 S74 之后的步骤中,读出器 / 写入器 12 向 CLF 77 发送 APDU 命令,例如认证请求命令、读出命令 (参考命令) 和写入命令 (更新命令)。CLF 77 向 VSE 小应用程序 74 供应从读出器 / 写入器 12 接收的 APDU 命令。VSE 小应用程序 74 向 SA 服务器 14 发送 APDU 命令。SA 服务器 14 执行与所发送的 APDU 命令中的每一个相对应的处理,并且发送响应 (处理的结果) 给 VSE 小应用程序 74。VSE 小应用程序 74 向 CLF77 供应从 SA 服务器 14 发送的响应。CLF 77 发送响应给读出器 / 写入器 12。

[0112] 以此方式,移动终端设备 11 (VSE 小应用程序 74) 操作为网关。因此,APDU 命令在读出器 / 写入器 12 与 SA 服务器 14 之间被传送,并且小应用程序在 SA 服务器 14 上被执行。因此,服务被提供给移动终端设备 11 的用户。

[0113] 在此时,用户以与先前相同的方式使移动终端设备 11 执行与读出器 / 写入器 12 的近场通信。以此方式,如用户接收移动终端设备 11 上执行的小应用程序所提供的服务的情况中那样,用户可接收 SA 服务器 14 上执行的小应用程序所提供的服务。

[0114] 通过上述处理,利用安全 ID 来认证移动终端设备 11。用于启动小应用程序的请求被从执行与所认证的移动终端设备 11 的近场通信的读出器 / 写入器 12 经由移动终端设备 11 发送到 SA 服务器 14。SA 服务器 14 识别被请求启动的并且与安全 ID 相对应的小应用程序所使用的用户数据项,并且利用所识别的数据项启动小应用程序。如上所述,因为用户数据项被存储在 SA 服务器 14 中并且小应用程序被执行,所以对移动终端设备 11 而言不必要存储用户数据项和执行小应用程序。因此,与近场通信相关的服务可被提供给用户,而不受移动终端设备 11 的平台以及移动终端设备 11 的处理能力和存储器的容量的限制。此外,因为利用作为关于移动终端设备 11 的认证信息的安全 ID 来管理用户数据项,所以可充分地确保用户数据项的安全性。结果,可以以安全的方式提供跨越所有终端设备的服务。

[0115] 此外,当用户数据项被存储在移动终端设备 11 中时,用于由内容提供者 (CP) 提供的小应用程序的用户数据项的存储区由于移动终端设备 11 的存储容量的限制而被限制。然而,在上述处理中,因为用户数据项被存储在具有大存储容量的 SA 服务器 14 中,所以由每个小应用程序使用的用户数据项的存储区可被灵活地分配。因此,可提供具有对所有内容提供者 (CP) 的公平性的系统。

[0116] 此外,在现有系统中,难以完全地管理由移动终端设备 11 执行的近场通信的日志 (事务日志)。然而,在上述配置中,事务日志等同于读出器 / 写入器 12 与 SA 服务器 14 之

间的通信的日志。因此,SA 服务器 14 可容易地管理所有的事务日志。以此方式,SA 服务器 14 可以辨认哪些服务被移动终端设备 11 的哪些用户使用。因此,例如,另外适合用户的偏好的服务可被提供。

[0117] 虽然已参考彼此分离的认证服务器 13 和 SA 服务器 14 来描述了以上实施例,但是认证服务器 13 和 SA 服务器 14 可如图 8 所示地被集成为一体。

[0118] 图 8 是示出包括认证服务器 13 的功能的 SA 服务器 14 的功能配置的示例的框图。注意,如以上在描述图 6 中的 SA 服务器 14 中所使用的,相同的名称和编号将被用在描述图 8 所示的 SA 服务器 14 中,并且对其的描述在适当的情况下不被重复。

[0119] 也就是说,从图 8 所示的 SA 服务器 14 可见,认证处理单元 131 被另外地设置在图 6 所示的 SA 服务器 14 中。注意,认证处理单元 131 具有与图 5 所示的认证服务器 13 的认证处理单元 92 的功能相同的功能。因此,对认证处理单元 131 的描述不在这里提供。

[0120] 注意,在图 8 所示的 SA 服务器 14 的配置中,不必要的是:在通过图 7 所示的流程图指示的处理中,在 VSE 小应用程序 74 被认证之后 SA 服务器 14 发送一次性 URL 给 VSE 小应用程序 74。

[0121] 此外,因为如上所述用户数据项被 SA 服务器 14 管理,所以除用户以外还可由内容提供者参考或更新用户数据项。

[0122] 下面描述用户或内容提供者可参考或更新 SA 服务器 14 中的用户数据项的信息处理系统的示例性配置。

[0123] <参考或更新用户数据的信息处理系统的示例性配置>

[0124] 图 9 示出用户或内容提供者可参考或更新 SA 服务器 14 中的用户数据项的信息处理系统的示例性配置。

[0125] 注意,如以上在描述图 1 中的信息处理系统中所使用的,相同的名称和编号将被用在描述图 9 所示的信息处理系统中,并且对其的描述在适当的情况下不被重复。

[0126] 也就是说,从图 9 所示的信息处理系统可见,读出器 / 写入器 12 被从图 1 所示的信息处理系统中去除,并且内容提供者 (CP) 服务器 151 被另外地设置在图 1 所示的信息处理系统中。

[0127] 移动终端设备 11 执行与基站 (未示出) 的无线通信,并且经由与基站连接的诸如因特网之类的网络与认证服务器 13 和 SA 服务器 14 通信。此外,移动终端设备 11 与 CP 服务器 151 通信。认证服务器 13、SA 服务器 14 和 CP 服务器 151 经由诸如因特网之类的网络彼此连接。

[0128] 响应于来自移动终端设备 11 的请求,CP 服务器 151 向移动终端设备 11 提供预定内容。此外,CP 服务器 151 发出用于访问 SA 服务器 14 的许可,并且发送该许可给移动终端设备 11 或认证服务器 13。如果许可被移动终端设备 11 或认证服务器 13 认证,则 CP 服务器 151 可访问 SA 服务器 14。

[0129] 下面描述图 9 所示的信息处理系统中执行的用于参考或更新用户数据项的处理。

[0130] <用于参考或更新用户数据的处理的示例 1>

[0131] 首先参考图 10 所示的流程图来描述由移动终端设备 11 的用户执行的、用于经由 CP 服务器 151 参考或更新 SA 服务器 14 中的用户数据项的处理。

[0132] 当用户使用移动终端设备 11 的 Web 浏览器并且请求 CP 服务器 151 发送所希望的

- 内容时,在步骤 S111 中 CP 服务器 151 向移动终端设备 11 发送与请求相对应的 Web 页面。
- [0133] 在步骤 S131 中,移动终端设备 11 从 CP 服务器 151 接收 Web 页面。在步骤 S132 中,移动终端设备 11 在 Web 浏览器中显示 Web 页面。
- [0134] 当用户操作移动终端设备 11 的 Web 浏览器中显示的 Web 页面以启动 VSE 小应用程序 74(例如,用户按压用于启动 VSE 小应用程序 74 的启动链接按钮)时,在步骤 S133 中,移动终端设备 11 启动 VSE 小应用程序 74。此时之后,在移动终端设备 11 中,VSE 小应用程序 74 起到 Web 浏览器的插件的作用。
- [0135] 随后,在步骤 S134 中,在获取 CP 服务器 151 的 URL 以访问 CP 服务器 151 之后,VSE 小应用程序 74 向 CP 服务器 151 发送对于允许 CP 服务器 151 访问 SA 服务器 14 的许可的请求(许可请求)。CP 服务器 151 的 URL 被存储在例如 Web 浏览器中显示的 Web 页面中的用于启动 VSE 小应用程序 74 的启动链接按钮中。
- [0136] 一在步骤 S112 中接收到来自 VSE 小应用程序 74 的许可请求,CP 服务器 151 就发出允许访问 SA 服务器 14 的许可。在步骤 S113 中,CP 服务器 151 发送许可给移动终端设备 11。注意,许可可被预先存储在 CP 服务器 151 中。
- [0137] 一在步骤 S135 中接收到来自 CP 服务器 151 的许可,移动终端设备 11 就在步骤 S136 中认证所接收的许可。如果许可被成功地认证,则移动终端设备 11 的 VSE 小应用程序 74 将移动终端设备 11 连接到认证服务器 13(步骤 S137 和步骤 S151)。在步骤 S152 中,认证服务器 13 的认证处理单元 92 经由 VSE 小应用程序 74 认证安全元件 76。以此方式,认证处理单元 92 认证移动终端设备 11。如果移动终端设备 11 被成功认证,则 VSE 小应用程序 74 访问安全元件 76 并且获取安全 ID。在步骤 S138 中,VSE 小应用程序 74 向认证服务器 13 发送所获取的安全 ID。
- [0138] 在步骤 S153 中,认证服务器 13 的通信单元 91 接收从移动终端设备 11 发送的安全 ID 并且将所接收的安全 ID 供应给认证处理单元 92。
- [0139] 在步骤 S153 中从通信单元 91 向认证处理单元 92 供应安全 ID 之后,认证处理单元 92 发出一次性 URL。
- [0140] 在步骤 S154 中,认证服务器 13 的通信单元 91 向移动终端设备 11 发送由认证处理单元 92 发出的一次性 URL。
- [0141] 一在步骤 S139 中接收到来自认证服务器 13 的一次性 URL,移动终端设备 11 的 VSE 小应用程序 74 就在步骤 S140 中发送连接请求给使用一次性 URL 的 SA 服务器 14。注意,连接请求包括安全 ID。
- [0142] 在步骤 S171 中,SA 服务器 14 的通信单元 111 从 VSE 小应用程序 74 接收连接请求。操作系统 112 利用从 VSE 小应用程序 74 发送的连接请求中所包括的安全 ID 来验证连接请求是从登录用户发送的。在步骤 S172 中,通信单元 111 向移动终端设备 11 发送对连接请求的响应。
- [0143] 一在步骤 S141 中接收到来自 SA 服务器 14 的响应,移动终端设备 11 的 VSE 小应用程序 74 就发送响应给 CP 服务器 151。在步骤 S114 中,CP 服务器 151 从 VSE 小应用程序 74 接收响应。以此方式,经由移动终端设备 11 的 CP 服务器 151 与 SA 服务器 14 之间的连接被建立。
- [0144] 在此时,如果用户操作移动终端设备 11 的 Web 浏览器中显示的 Web 页面以参考或

更新用户数据项,则在步骤 S115 中,CP 服务器 151 向移动终端设备 11 发送用于参考或更新用户数据项的请求命令。请求命令包括用于识别用于参考或更新用户数据项的小应用程序的 AID。

[0145] 在步骤 S142 中,移动终端设备 11 从 CP 服务器 151 接收请求命令并且利用 TCAP 向 SA 服务器 14 发送所接收的请求命令。在此时,请求命令包括移动终端设备 11 的安全 ID。

[0146] 一在步骤 S173 中接收到来自移动终端设备 11 的请求命令,SA 服务器 14 就在步骤 S174 中参考或更新通过请求命令中包括的安全 ID 和 AID 识别的用户数据项。

[0147] 在步骤 S175 中,SA 服务器 14 利用 TCAP 向移动终端设备 11 发送对请求命令的响应。

[0148] 一在步骤 S143 中接收到来自 SA 服务器 14 的响应,移动终端设备 11 就发送所接收的响应给 CP 服务器 151。

[0149] 一在步骤 S116 中接收到来自移动终端设备 11 的响应,CP 服务器 151 就向移动终端设备 11 以 Web 页面的形式发送与响应相对应的信息。

[0150] 注意,从 CP 服务器 151 发送的请求命令是读出命令(参考命令)或写入命令(更新命令)。更具体地,当移动终端设备 11 的用户请求参考用户数据项时,CP 服务器 151 向 SA 服务器 14 发送读出命令,并且 SA 服务器 14 向 CP 服务器 151 发送对读出命令的响应。此外,当移动终端设备 11 的用户请求更新用户数据项时,CP 服务器 151 请求参考用户数据项并且接收对请求的响应。此后,CP 服务器 151 发送写入命令给 SA 服务器 14。SA 服务器 14 向 CP 服务器 151 发送对写入命令的响应。

[0151] 注意,在移动终端设备 11 中,VSE 小应用程序 74 执行作为脚本的、根据从 CP 服务器 151 接收的命令的处理。在此时,移动终端设备 11 与 SA 服务器 14 之间被传送的命令符合 APDU 命令格式是必要的。然而,移动终端设备 11 与 CP 服务器 151 之间被传送的命令可以不符合 APDU 命令格式。

[0152] 以此方式,移动终端设备 11 的用户可经由 CP 服务器 151 参考或更新 SA 服务器 14 中的用户数据项。

[0153] 虽然已参考经由移动终端设备 11 向 SA 服务器 14 发送请求命令的 CP 服务器 151 进行了以上描述,但是 CP 服务器 151 可直接发送请求命令给 SA 服务器 14。

[0154] <用于参考或更新用户数据的处理的示例 2>

[0155] 接下来参考图 11 所示的流程图来描述移动终端设备 11 的用户经由向 SA 服务器 14 直接发送请求命令的 CP 服务器 151 来参考或更新 SA 服务器 14 中的用户数据项的处理。

[0156] 注意,在图 11 所示的流程图中,由 CP 服务器 151 执行的步骤 S211 到 S213、由移动终端设备 11 执行的步骤 S231 到 S238、以及由认证服务器 13 执行的步骤 S251 到 S254 分别类似于图 10 所示的流程图中的由 CP 服务器 151 执行的步骤 S111 到 S113、由移动终端设备 11 执行的步骤 S131 到 S138、以及由认证服务器 13 执行的步骤 S151 到 S154。因此,对其的描述不被重复。

[0157] 也就是说,一接收到来自认证服务器 13 的一次性 URL,移动终端设备 11 的 VSE 小应用程序 74 就在步骤 S239 中将从安全元件获取的安全 ID 与一次性 URL 一起发送给 CP 服务器 151。

[0158] 一在步骤 S214 中接收到来自移动终端设备 11 的一次性 URL 和安全 ID,CP 服务器

151 就在步骤 S215 中基于一次性 URL 向 SA 服务器 14 发送连接请求。注意,连接请求包括安全 ID。

[0159] 在步骤 S271 中,SA 服务器 14 的通信单元 111 从 CP 服务器 151 接收连接请求。操作系统 112 基于来自 CP 服务器 151 的连接请求中包括的安全 ID 来认证 CP 服务器 151。在步骤 S272 中,通信单元 111 向 CP 服务器 151 发送对连接请求的响应。在步骤 S216 中,CP 服务器 151 从 VSE 小应用程序 74 接收响应。以此方式,CP 服务器 151 与 SA 服务器 14 之间的连接被建立。

[0160] 在此时,如果用户操作移动终端设备 11 的 Web 浏览器中显示的 Web 页面以参考或更新用户数据项,则在步骤 S217 中,CP 服务器 151 利用 TCAP 向 SA 服务器 14 发送用于参考或更新用户数据项的请求命令。请求命令包括移动终端设备 11 的安全 ID 和用于识别用于参考或更新用户数据项的小应用程序的 AID。

[0161] 一在步骤 S273 中接收到来自 CP 服务器 151 的请求命令,SA 服务器 14 就在步骤 S274 中参考或更新通过请求命令中包括的安全 ID 和 AID 识别的用户数据项。

[0162] 在步骤 S275 中,SA 服务器 14 利用 TCAP 向 CP 服务器 151 发送对请求命令的响应。

[0163] 一在步骤 S218 中接收到来自 SA 服务器 14 的对请求命令的响应,CP 服务器 151 就向移动终端设备 11 以 Web 页面的形式发送与响应相对应的信息。

[0164] 注意,CP 服务器 151 与 SA 服务器 14 之间被传送的命令符合 APDU 命令格式。

[0165] 如上所述,即使当 CP 服务器 151 直接发送请求命令给 SA 服务器 14 时,移动终端设备 11 的用户也可经由 CP 服务器 151 参考或更新 SA 服务器 14 中的用户数据项。

[0166] 虽然已参考移动终端设备 11 的用户经由 CP 服务器 151 参考或更新 SA 服务器 14 中的用户数据项的处理进行了以上的描述,但是拥有 CP 服务器 151 的内容提供者 (CP) 可参考或更新 SA 服务器 14 中的用户数据项。

[0167] <用于参考或更新用户数据的处理的示例 3>

[0168] 接下来参考图 12 所示的流程图来描述拥有 CP 服务器 151 的 CP 参考或更新 SA 服务器 14 中的用户数据项的处理。

[0169] 当 CP 服务器 151 连接到认证服务器 13 时,在步骤 S331 中,认证服务器 13 向 CP 服务器 151 发送对许可的请求。

[0170] 一在步骤 S311 中接收到来自认证服务器 13 的对许可的请求,CP 服务器 151 就发出用于访问 SA 服务器 14 的许可。在步骤 S312 中,CP 服务器 151 向认证服务器 13 发送许可。

[0171] 一在步骤 S332 中接收到来自 CP 服务器 151 的许可,认证服务器 13 就在步骤 S333 中认证所接收的许可。如果许可被成功地认证,则认证服务器 13 的认证处理单元 92 发出一次性 URL。

[0172] 在步骤 S334 中,认证服务器 13 的通信单元 91 向 CP 服务器 151 发送由认证处理单元 92 发出的一次性 URL。

[0173] 一在步骤 S313 中接收到来自认证服务器 13 的一次性 URL,CP 服务器 151 就在步骤 S314 中基于一次性 URL 向 SA 服务器 14 发送连接请求。

[0174] 一在步骤 S351 中接收到来自 CP 服务器 151 的连接请求,SA 服务器 14 的通信单元 111 就在步骤 S352 中向 CP 服务器 151 发送对连接请求的响应。在步骤 S315 中,CP 服

务器 151 从 SA 服务器 14 接收响应。以此方式,CP 服务器 151 与 SA 服务器 14 之间的连接被建立。

[0175] 在此时,如果 CP 对 CP 服务器 151 执行操作以参考或更新用于特定小应用程序的用户数据项,则在步骤 S316 中,CP 服务器 151 利用 TCAP 向 SA 服务器 14 发送用于参考或更新用户数据项的请求命令。请求命令包括用于识别特定小应用程序的 AID。

[0176] 一在步骤 S353 中接收到来自 CP 服务器 151 的请求命令,SA 服务器 14 就在步骤 S354 中参考或更新通过请求命令中包括的 AID 来识别的用户数据项。在此时,被参考或更新的用户数据项可被特定小应用程序使用。与多个安全 ID(多个移动终端设备 11,即多个用户)相对应的用户数据项可被参考或更新。

[0177] 在步骤 S355 中,SA 服务器 14 利用 TCAP 向 CP 服务器 151 发送对请求命令的响应。

[0178] 一在步骤 S317 中接收到来自 SA 服务器 14 的对请求命令的响应,CP 服务器 151 就向例如 CP 服务器 151 的显示单元(未示出)输出与响应相对应的信息。

[0179] 以此方式,拥有 CP 服务器 151 的内容提供者可以直接地参考或更新 SA 服务器 14 中的用户数据项。因此,内容提供者可以容易地辨认现有系统中的个别用户的移动终端设备 11 中所存储的用户数据项。因此,例如,内容提供者可基于统计的用户数据来提供新服务。此外,内容提供者可通过与其他内容提供者共享用户数据项来提供多种多样的服务。

[0180] 已参考图 1 所示的可以向使用移动终端设备 11 的用户提供诸如电子货币服务、检票服务、考勤服务或门禁管理服务之类的服务的信息处理系统进行了以上描述。

[0181] 然而,根据图 7 所示的处理,从来自读出器/写入器 12 的请求被发送给 SA 服务器 14 的时刻到请求被读出器/写入器 12 接收的时刻花费了某个时间。因此,难以将处理应用于诸如检票服务之类的高速服务。

[0182] 下面描述适用于高速服务的配置和处理。

[0183] <信息处理系统的配置的另一示例>

[0184] 图 13 是具体地在火车站中向移动终端设备 11 的用户提供检票服务的信息处理系统的框图。

[0185] 注意,如以上在描述图 1 中的信息处理系统中所使用的,相同的名称和编号将被用在描述图 13 中的信息处理系统中,并且对其的描述在适当的情况下不被重复。

[0186] 也就是说,从图 13 所示的信息处理系统可见,认证服务器 13 被从图 1 所示的信息处理系统中去除,并且车站服务器 171 被另外地设置。

[0187] 注意,读出器/写入器 12 被配置为诸如自动检票口之类的车站服务设备的一部分。读出器/写入器 12 与车站服务器 171 连接。

[0188] 车站服务器 171 管理通过包括读出器/写入器 12 的车站服务设备所执行的处理而获得的信息。当必要时,车站服务器 171 供应信息给 SA 服务器 14。SA 服务器 14 和车站服务器 171 经由诸如因特网或内联网之类的网络而彼此连接。

[0189] 注意,SA 服务器 14 类似于图 8 所示的并且包括认证服务器 13 的功能的 SA 服务器 14。

[0190] <用于提供高速服务的处理的示例>

[0191] 接下来参考图 14 所示的流程图来描述用于提供由图 13 所示的信息处理系统执行的服务的处理的示例。

[0192] 例如,如果用户轻敲移动终端设备 11 的显示画面上显示的 VSE 小应用程序 74 的图标,则在步骤 S411 中,移动终端设备 11 启动 VSE 小应用程序 74。VSE 小应用程序 74 将移动终端设备 11 连接到 SA 服务器 14(步骤 S412 和步骤 S431)。在步骤 S432 中,SA 服务器 14 的认证处理单元 131 经由 VSE 小应用程序 74 认证安全元件 76 并且认证移动终端设备 11。如果移动终端设备 11 被成功地认证,则 VSE 小应用程序 74 访问安全元件 76 并且获取安全 ID。

[0193] 在步骤 S413 中,VSE 小应用程序 74 经由通信单元 75、基站和诸如因特网之类的网络向 SA 服务器 14 发送(供应)所获取的安全 ID。此外,VSE 小应用程序 74 发送对于与安全 ID 相对应的用户数据项的请求。

[0194] 在步骤 S433 中,SA 服务器 14 的通信单元 111 接收经由诸如因特网之类的网络从移动终端设备 11 发送的安全 ID,并且将所接收的安全 ID 供应给操作系统 112。

[0195] 在步骤 S434 中,响应于对于与安全 ID 相对应的用户数据项的请求,操作系统 112 的数据管理模块 112a 在个人化 DB 113 中识别与安全 ID 相对应的用户数据项并且将用户数据项的副本供应给通信单元 111。在此时,数据管理模块 112a 利用签名来加密用户数据项的副本。此外,为了记录此时刻,数据管理模块 112a 可将加密的时刻附加至个人化 DB 113 中被识别的用户数据项以及用户数据项的副本。

[0196] 在步骤 S434 中,通信单元 111 向 VSE 小应用程序 74 发送由数据管理模块 112a 识别的用户数据项的副本。

[0197] 一接收到来自 SA 服务器 14 的用户数据项的副本,VSE 小应用程序 74 就在步骤 S414 中向中间件 73 供应用户数据项的副本。在步骤 S451 中,中间件 73 获取从 VSE 小应用程序 74 发送的用户数据项的副本。在步骤 S452 中,中间件 73 将用户数据项的副本缓存在存储区(未示出)中。

[0198] 在此时,在移动终端设备 11 中,用户数据项的副本可被临时地存储在存储区(未示出)中。可替代地,用户数据项的副本可以以持久数据的形式而被存储。此后,每次新的用户数据项被从 SA 服务器 14 发送时,持久数据可被更新。

[0199] 此外,在步骤 S415 中,VSE 小应用程序 74 激活移动终端设备 11。更具体地,VSE 小应用程序 74 改变移动终端设备 11 的显示画面的显示颜色并且使 CLF 77 进入近场通信的待机模式。

[0200] 在此时,因为移动终端设备 11 的显示画面的显示颜色被改变,所以用户辨认出移动终端设备 11 可执行近场通信并且将移动终端设备 11 移到被集成进自动检票口的读出器/写入器 12 上(将移动终端设备 11 移动得较接近读出器/写入器 12)。

[0201] 虽然未示出,但是如果移动终端设备 11 接近读出器/写入器 12,则读出器/写入器 12 向 CLF 77 发送轮询并且 CLF 77 向读出器/写入器 12 返回对轮询的响应。也就是说,读出器/写入器 12 辨认了用作通信伙伴的移动终端设备 11。

[0202] 在步骤 S471 中,读出器/写入器 12 向 CLF 77 发送用于识别系统的系统代码。在此情况下,所发送的系统代码指示其中移动终端设备 11 被使用的系统是检票系统。

[0203] 一接收到来自读出器/写入器 12 的系统代码,CLF 77 就在步骤 S491 中供应系统代码给中间件 73。

[0204] 一在步骤 S453 中接收到来自 CLF 77 的系统代码,中间件 73 就在步骤 S454 中进

入仿真 (emulation) 模式。因此,中间件 73 可执行与检票处理相关的处理。注意,代替发送系统代码地,读出器 / 写入器 12 可发送用于中间件 73 对执行与检票处理相关的小应用程序进行仿真的信息。例如,作为 APDU 命令之一的上述选择 (AID) 可从读出器 / 写入器 12 被发送。

[0205] 虽然已参考对用于执行与检票处理相关的小应用程序进行仿真的中间件 73 来进行了以上描述,但是 VSE 小应用程序 74 可对用于执行与检票处理相关的小应用程序进行仿真。

[0206] 随后,在步骤 S455 中,中间件 73 向 CLF 77 供应对系统代码的响应。一接收到来自中间件 73 的响应,CLF 77 就在步骤 S492 中向读出器 / 写入器 12 发送响应。

[0207] 一在步骤 S472 中接收到来自 CLF 77 的响应,读出器 / 写入器 12 就在步骤 S473 中发送对用户数据项的读出请求 (读出命令)。一接收到来自读出器 / 写入器 12 的读出请求,CLF 77 就在步骤 S493 中发送读出请求给中间件 73。

[0208] 一在步骤 S456 中接收到来自 CLF 77 的读出请求,中间件 73 就在步骤 S457 中将存储区 (未示出) 中缓存的具有签名的用户数据项的副本供应给 CLF 77 作为对读出请求的响应。

[0209] 一在步骤 S494 中接收到来自中间件 73 的响应 (用户数据项的副本),CLF 77 就发送响应给读出器 / 写入器 12。

[0210] 一在步骤 S474 中接收到来自 CLF 77 的响应,读出器 / 写入器 12 就在步骤 S475 中执行用于打开 / 关闭自动检票口的处理。此外,如果用户数据项的副本包括签名和时间戳,则读出器 / 写入器 12 可验证签名和时间戳并且根据验证的结果来执行用于打开 / 关闭自动检票口的处理。

[0211] 以此方式,移动终端设备 11 的用户可通过将移动终端设备 11 移到被集成进自动检票口的读出器 / 写入器 12 上来经过自动检票口。

[0212] 在步骤 S476 中,读出器 / 写入器 12 基于来自 CLF 77 的响应 (用户数据项的副本) 而向车站服务器 171 供应对 SA 服务器 14 中存储的用户数据项的写入请求。在此情况下,写入请求包括上述签名。

[0213] 一在步骤 S511 中获取了来自读出器 / 写入器 12 的写入请求,车站服务器 171 就在步骤 S512 中发送写入请求给 SA 服务器 14。注意,在向 SA 服务器 14 发送写入请求之前,车站服务器 171 可发送认证请求给 SA 服务器 14 并且接收对认证请求的响应。此后,车站服务器 171 可发送写入请求给 SA 服务器 14。

[0214] 一在步骤 S435 中接收到来自车站服务器 171 的写入请求,SA 服务器 14 就在步骤 S436 中利用附于写入请求上的签名来更新具有签名的用户数据项。更具体地,作为用户数据项而存储在个人化 DB 113 中的电子货币的结存信息被更新成减了移动终端设备 11 的用户支付的运费的结存信息。注意,如果用户数据项包括时刻信息,则 SA 服务器 14 可基于时刻信息和 SA 服务器 14 接收来自车站服务器 171 的写入请求的时刻来验证用户数据项的完整性。

[0215] 根据上述处理,SA 服务器 14 中存储的用户数据项的副本被缓存在移动终端设备 11 中,并且与近场通信相关的处理是基于用户数据项的副本由移动终端设备 11 而不是 SA 服务器 14 来执行的。因此,可提供诸如检票服务之类的高速服务。

[0216] 注意,来自车站服务器 171 进行的写入请求的发送以及 SA 服务器 14 进行的用户数据项的更新的处理被实时地执行是不必要的。该处理可以以批量模式来执行。

[0217] 虽然已参考作为移动终端设备 11 的认证信息的安全元件 76 的安全 ID 来描述了实施例,但是安全地认证移动终端设备 11 的任何信息可被使用。例如,如果移动终端设备 11 是蜂窝电话,则电话号码可被用作认证信息。如果移动终端设备 11 包括诸如指纹认证功能之类的生物测定 (biometric) 认证功能,则生物测定信息可被用作认证信息。可替代地,用于存储现有移动终端设备 11 中执行的小应用程序的通用集成电路卡 (UICC) 所特有的信息可被用作认证信息。

[0218] 此外,虽然已参考由 ISO 18092 定义的利用 Type A 或 Type B 方法的在移动终端设备 11 与读出器 / 写入器 12 之间执行的近场通信来描述了实施例,但是除了 Type A 或 Type B 方法以外的方法可被使用。此外,移动终端设备 11 与读出器 / 写入器 12 之间执行的近场通信可以是利用端子的接触式通信而不是非接触式通信。

[0219] 此外,虽然已参考包括单个 SA 服务器 14 的信息处理系统来描述了以上实施例,但是可为小应用程序中的每一个 (即提供小应用程序的内容提供者中的每一个) 都设置 SA 服务器。

[0220] 此外,虽然已参考具有多个功能的 VSE 小应用程序 74 来描述了以上实施例,但是多个 VSE 小应用程序 74 中的每一个都可具有它自己的功能。

[0221] 上述系列的处理不仅可由硬件而且可由软件来执行。当上述系列的处理由软件执行时,软件的程序被从程序记录介质安装进结合在专用硬件中的计算机或者可通过在其中安装各种程序来执行各种功能的计算机 (例如,通用个人计算机) 之中。

[0222] 如图 3 所示,存储要安装在计算机中的以及要由计算机执行的程序的程序记录介质是从作为被封装介质的可移除介质 61、临时地或永久地存储程序的 RAM 53、或者永久地存储程序的 ROM 52 或硬盘形成的。可移除介质 61 的示例包括磁盘 (包括柔性盘)、光盘 (包括 CD-ROM (光碟 - 只读存储器)、DVD (数字多功能光碟) 和磁光盘)、或者半导体盘。当必要时,利用诸如网络、局域网、因特网或数字广播之类的有线或无线通信介质,经由用作诸如路由器或调制解调器之类的接口的通信单元 (未示出) 而在程序记录介质中存储程序。

[0223] 此外,由计算机执行的程序可以是以上述次序执行处理的程序或者并行地或按照需求来执行处理的程序。

[0224] 本领域的技术人员应当理解,本公开的实施例不限于上述实施例,并且可在所附权利要求或其等同物的范围内进行各种修改。

[0225] 本公开包含与 2010 年 12 月 8 日递交日本专利局的日本优先专利申请 JP 2010-273189 中所公开的主题相关的主题,该日本优先专利申请的全部内容由此通过引用而被结合。

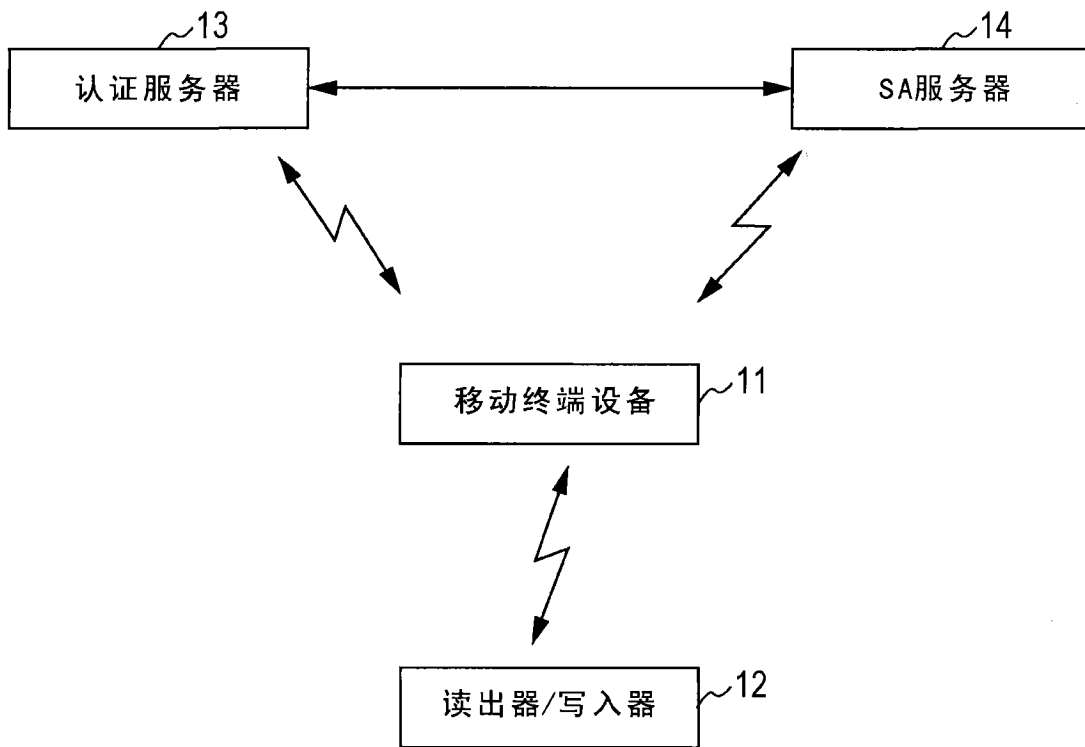


图 1

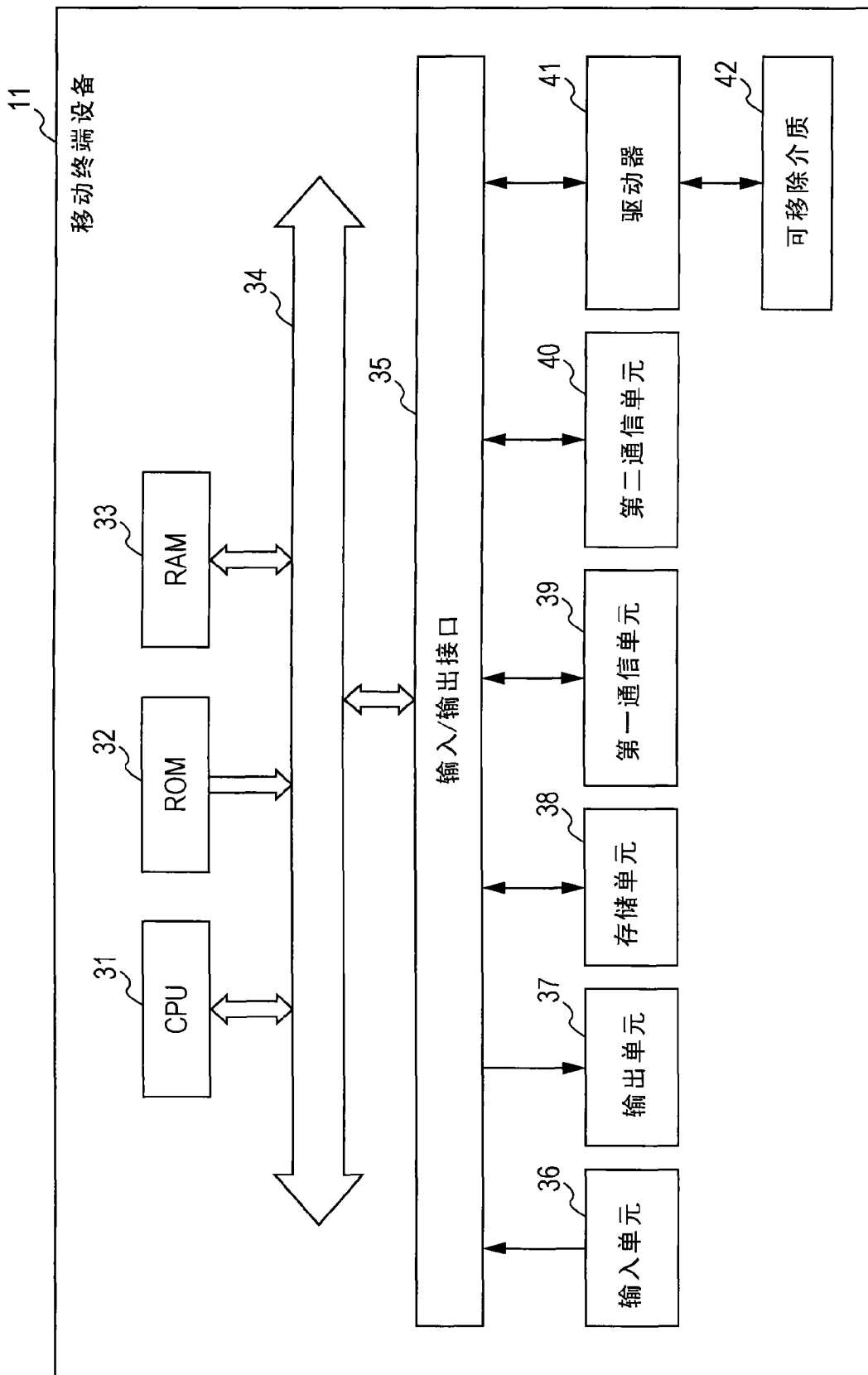


图 2

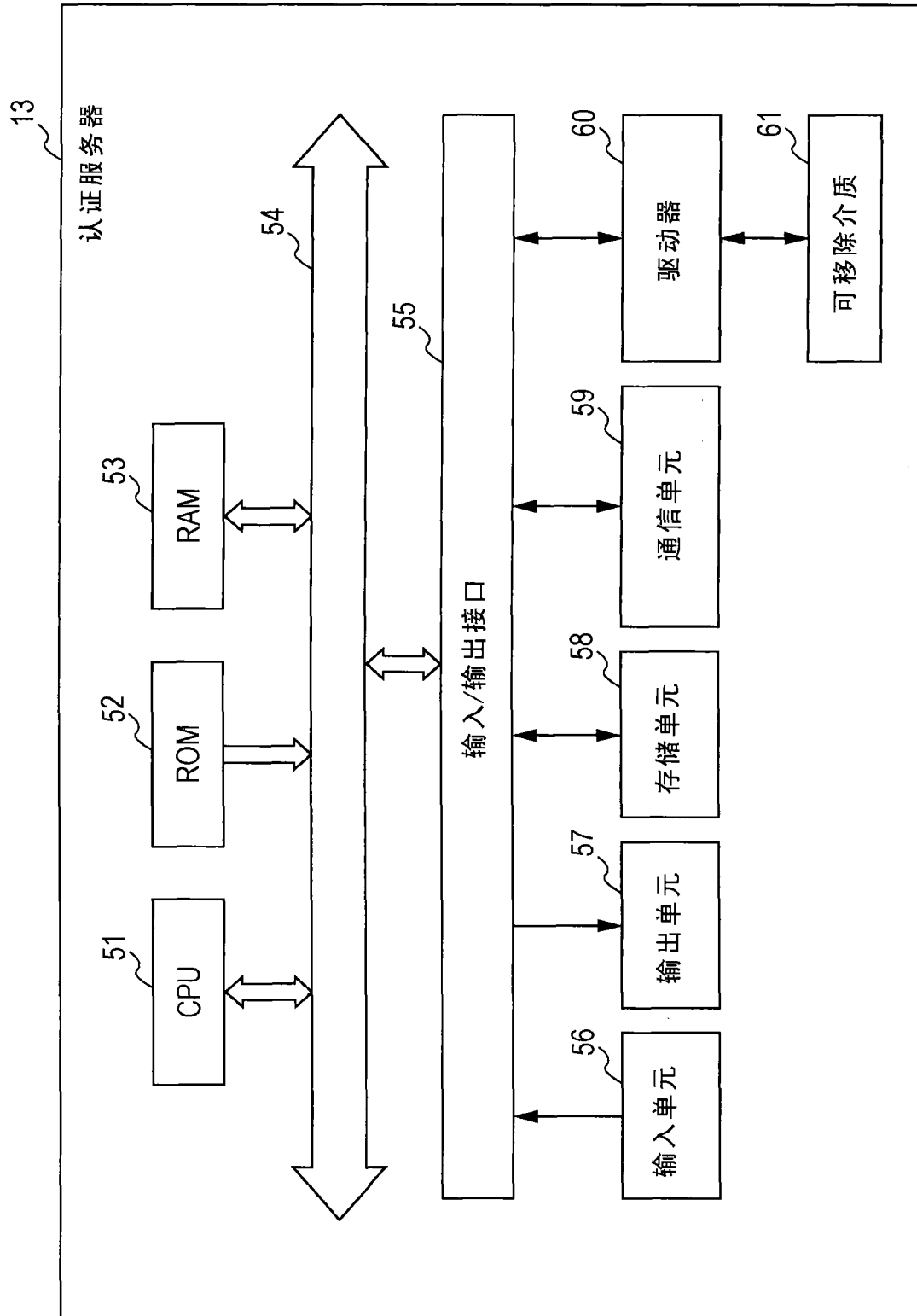


图 3

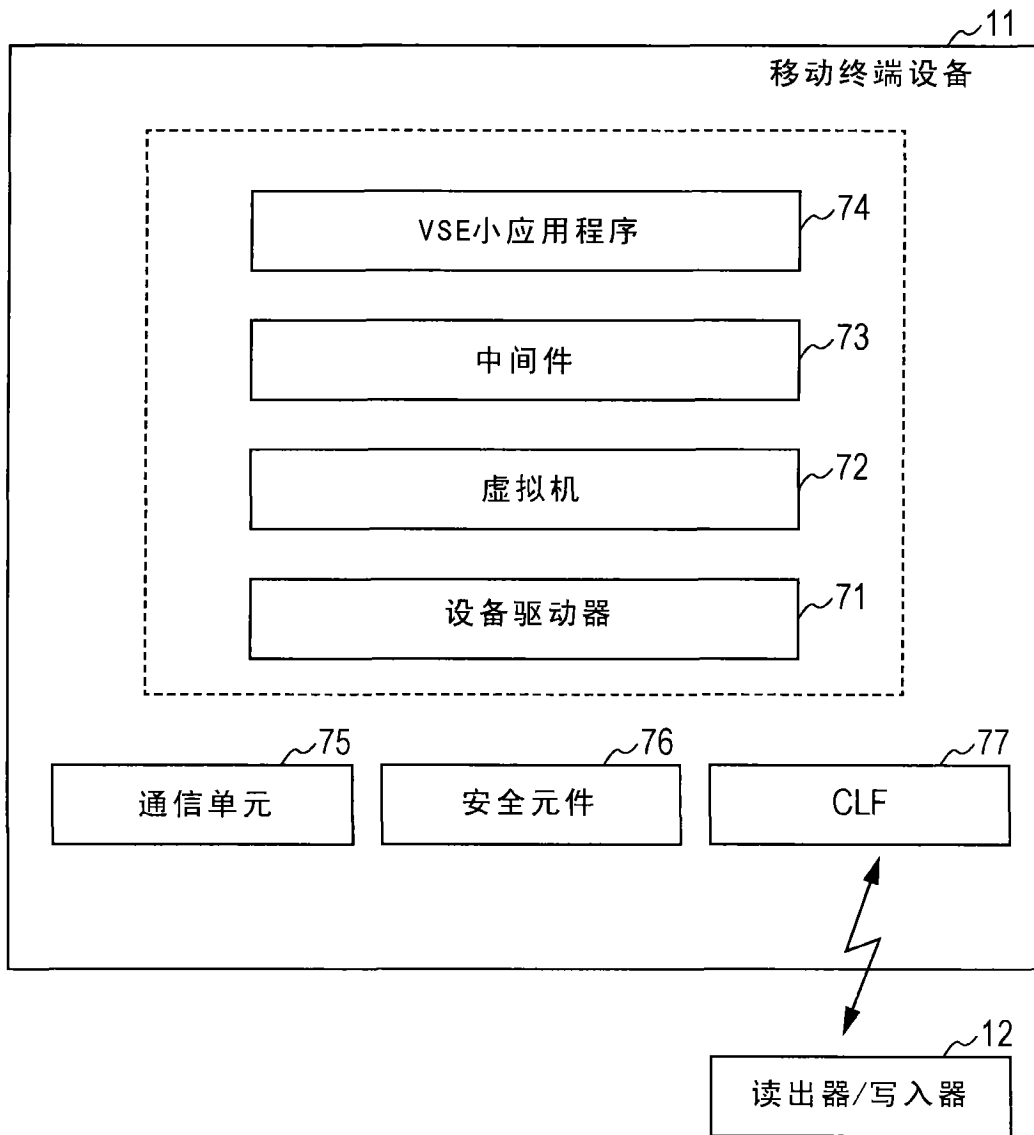


图 4

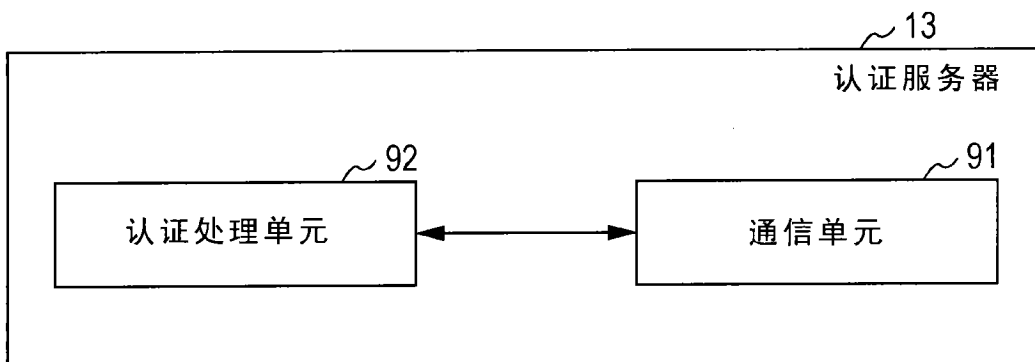


图 5

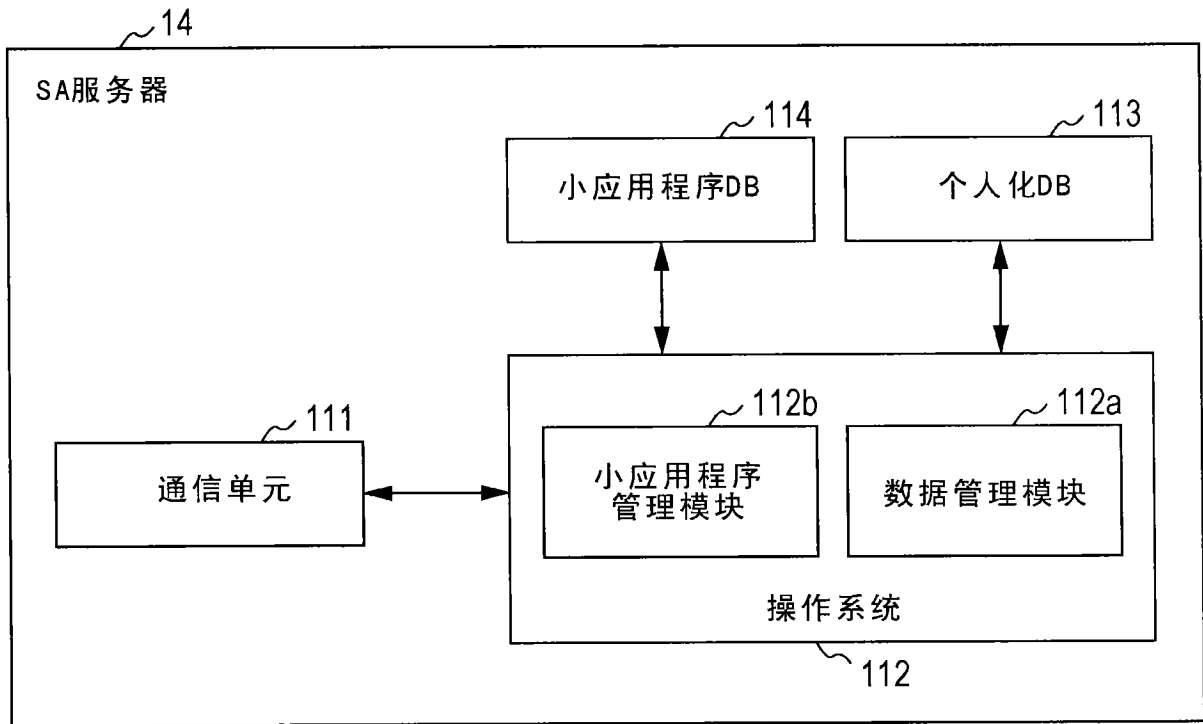


图 6

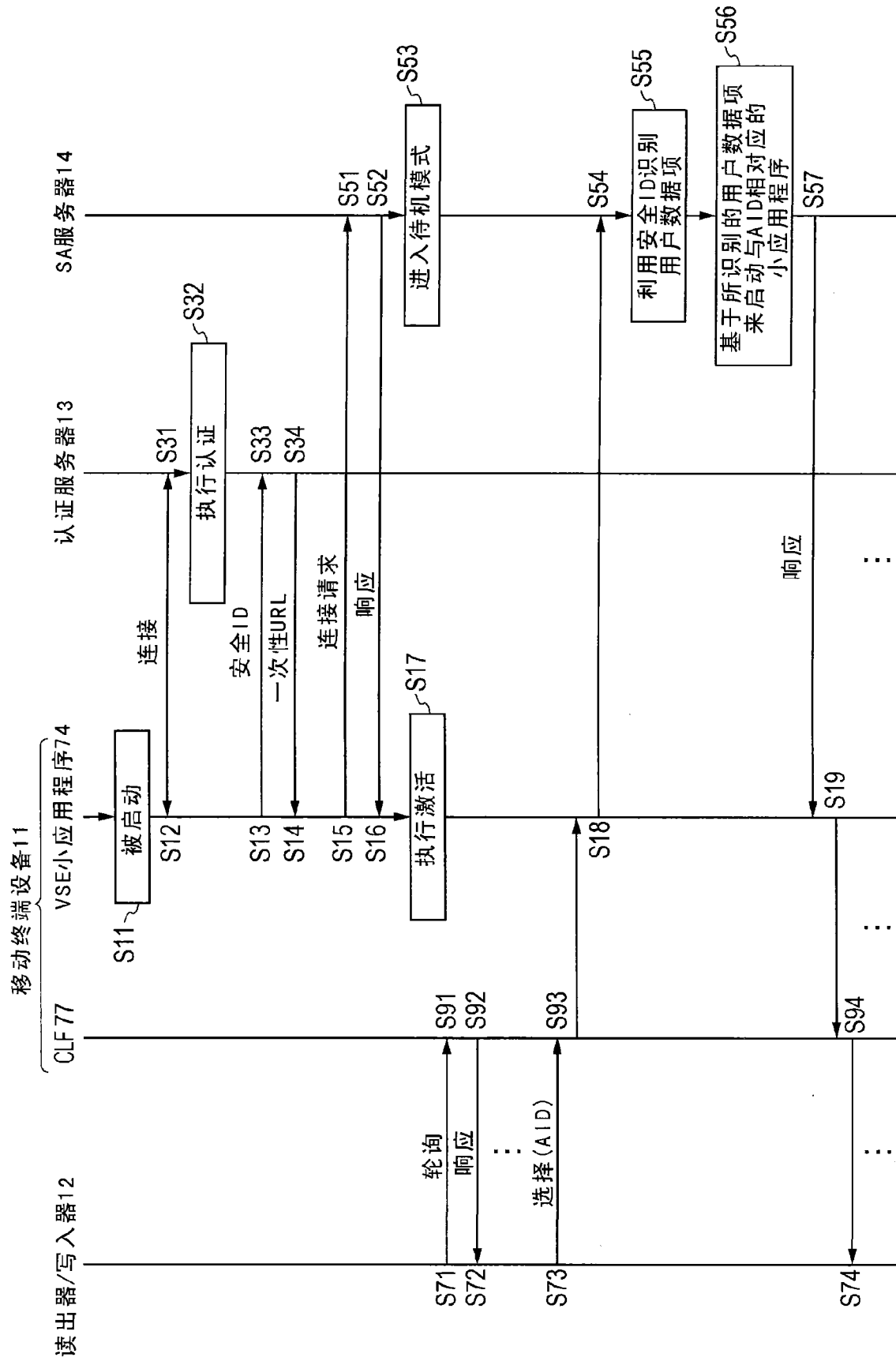


图 7

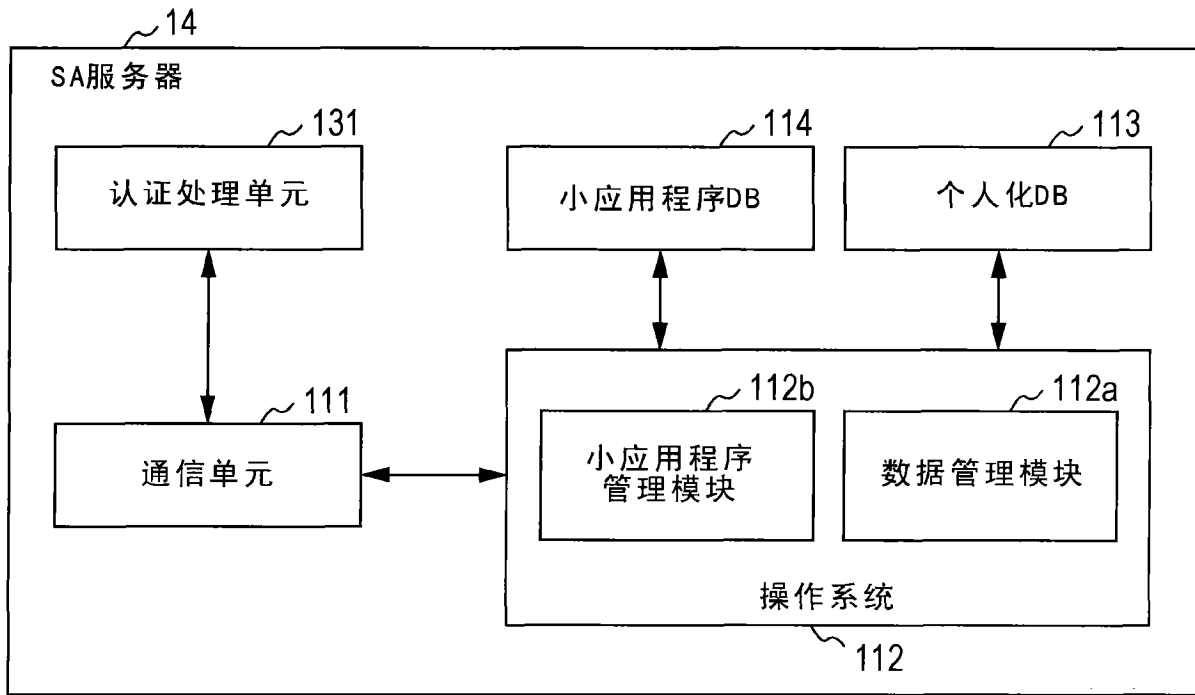


图 8

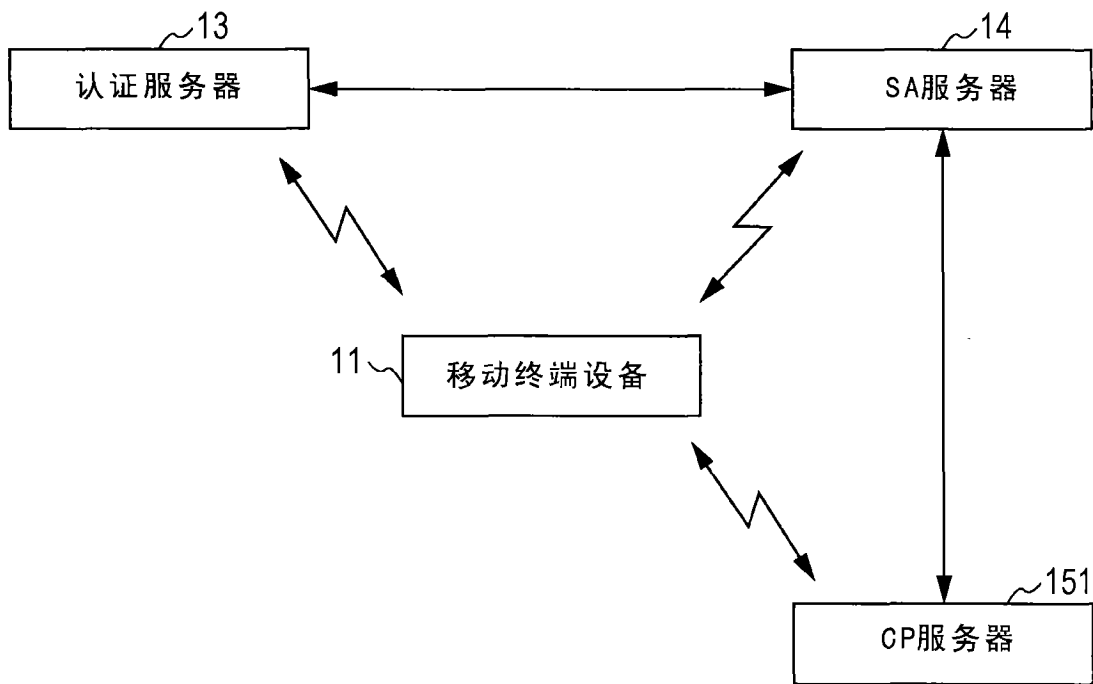


图 9

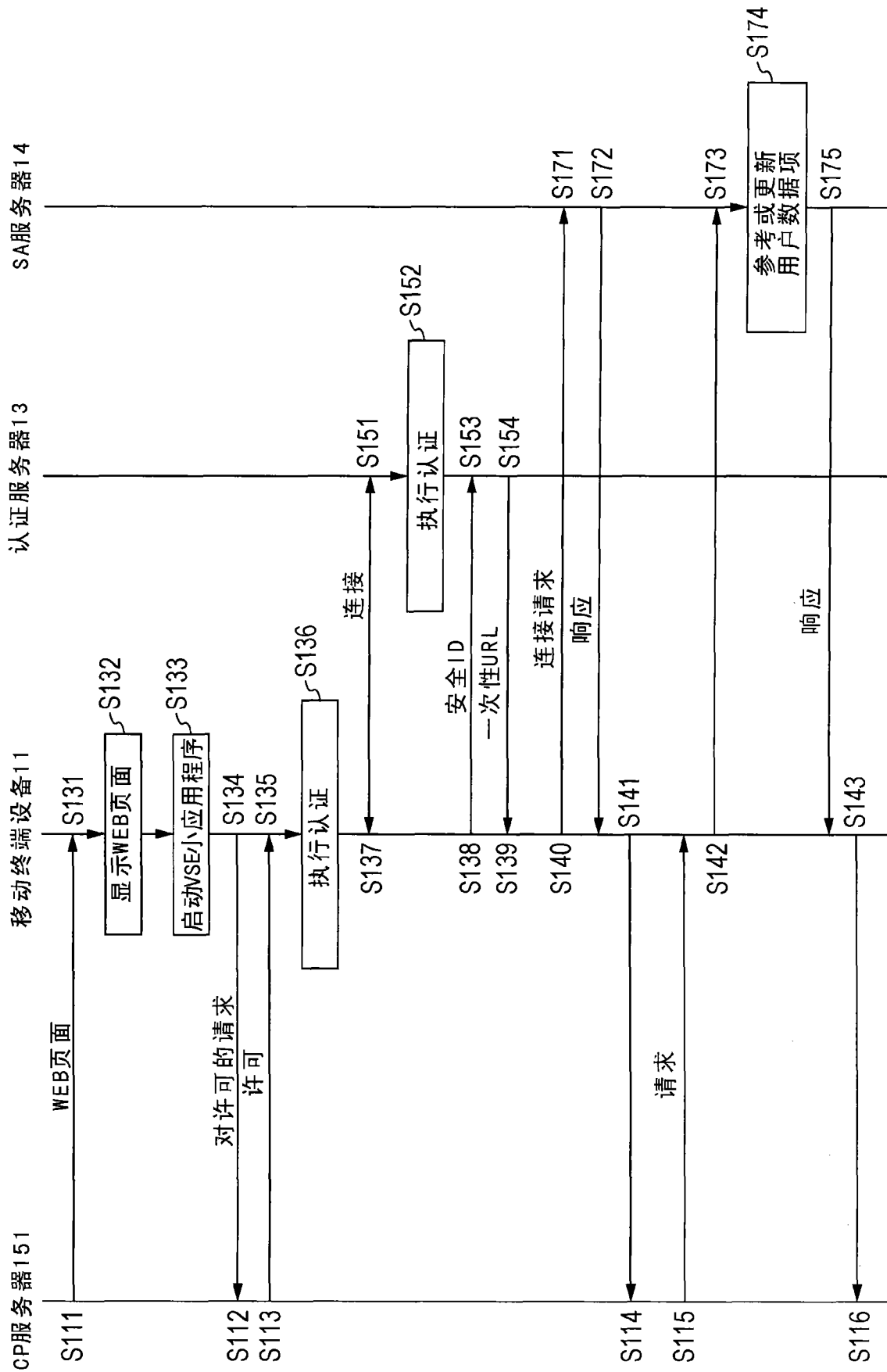


图 10

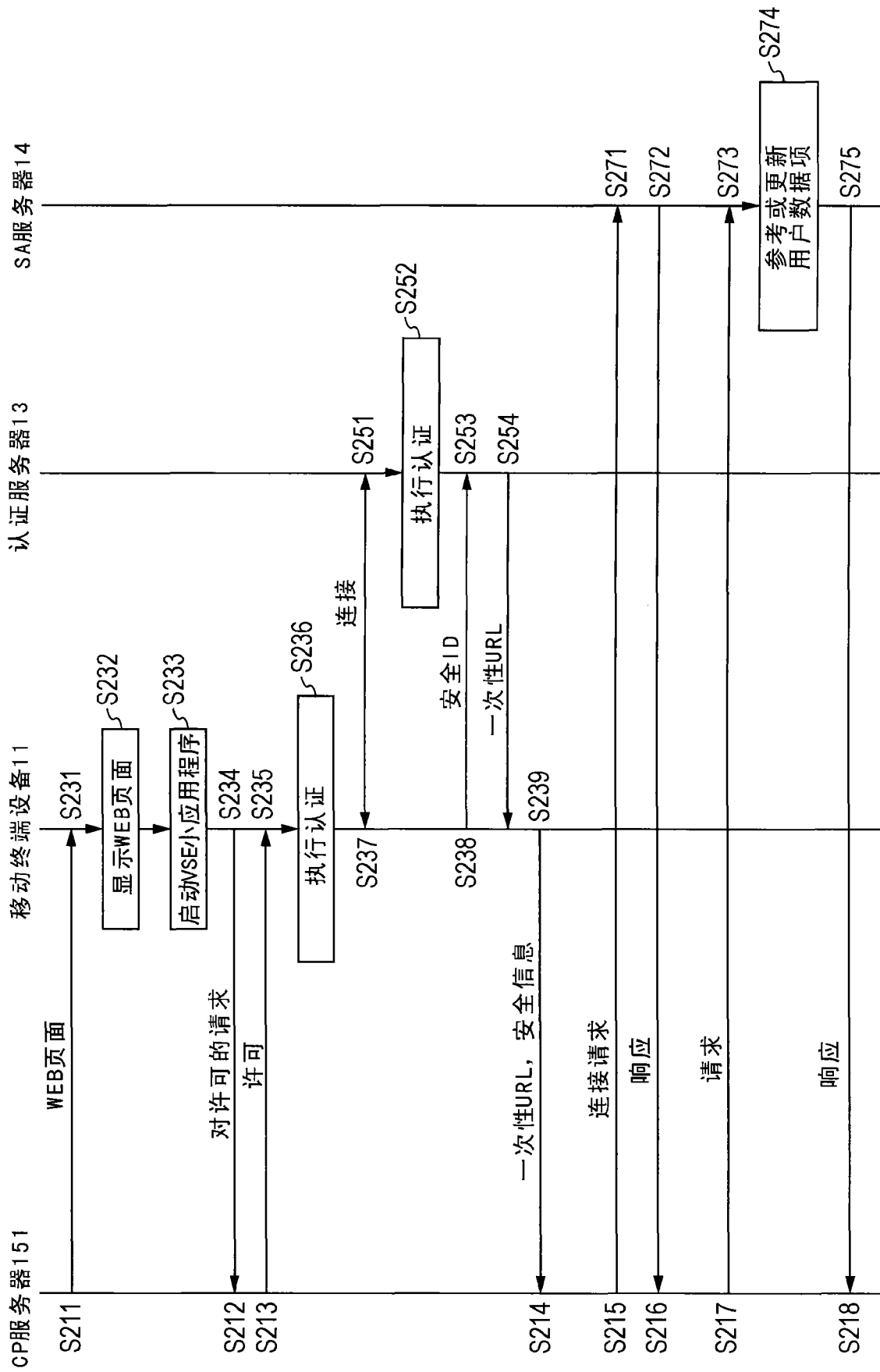


图 11

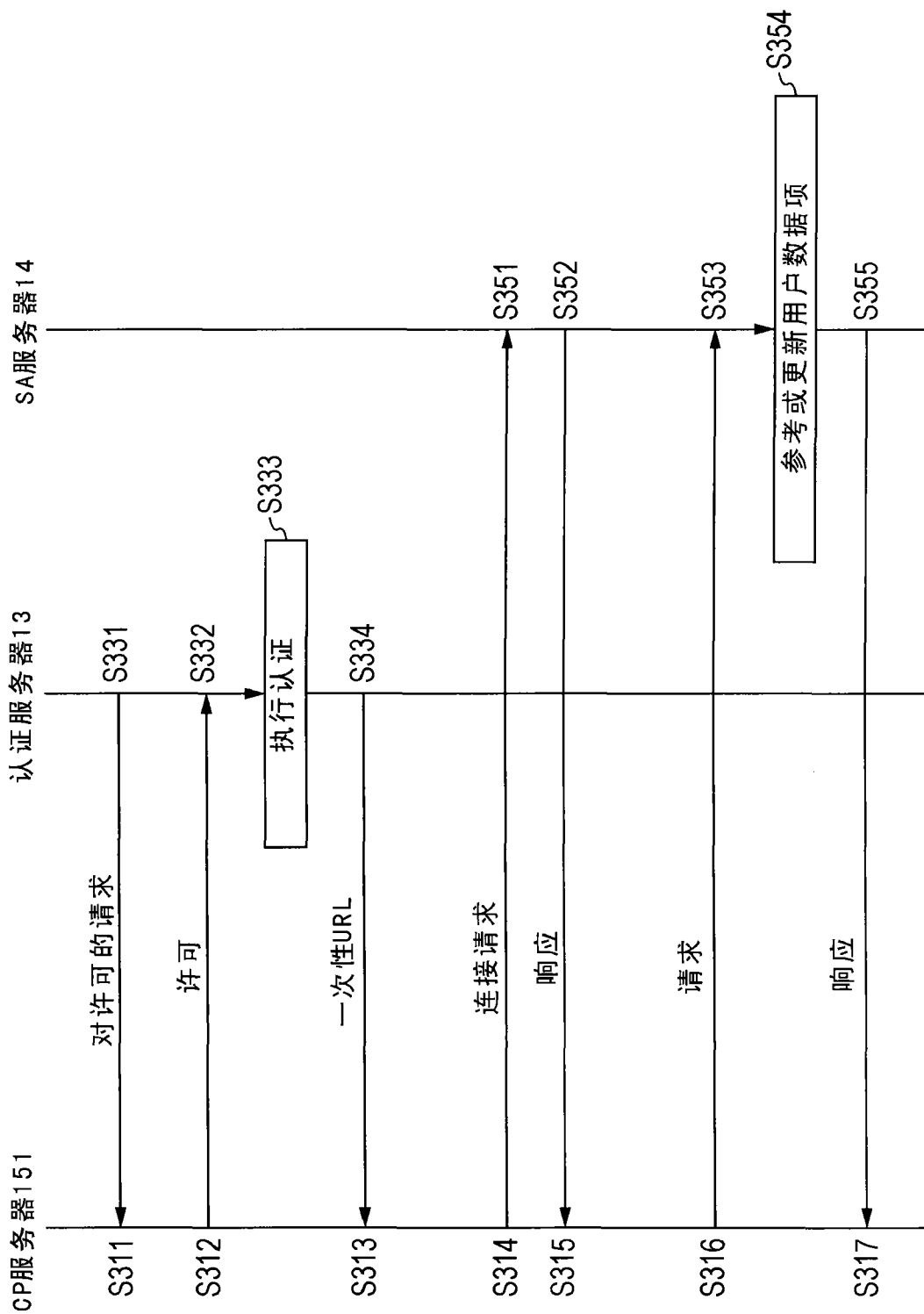


图 12

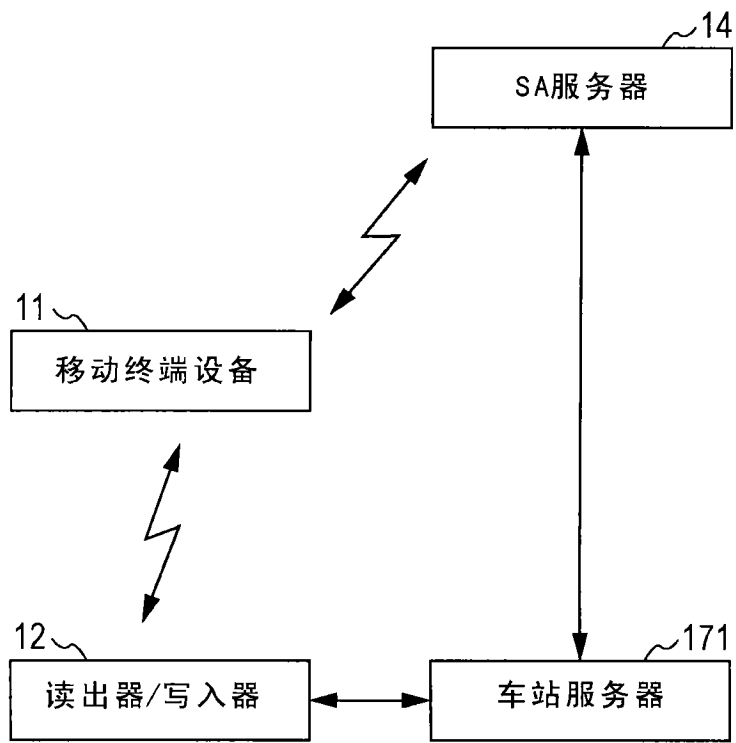


图 13

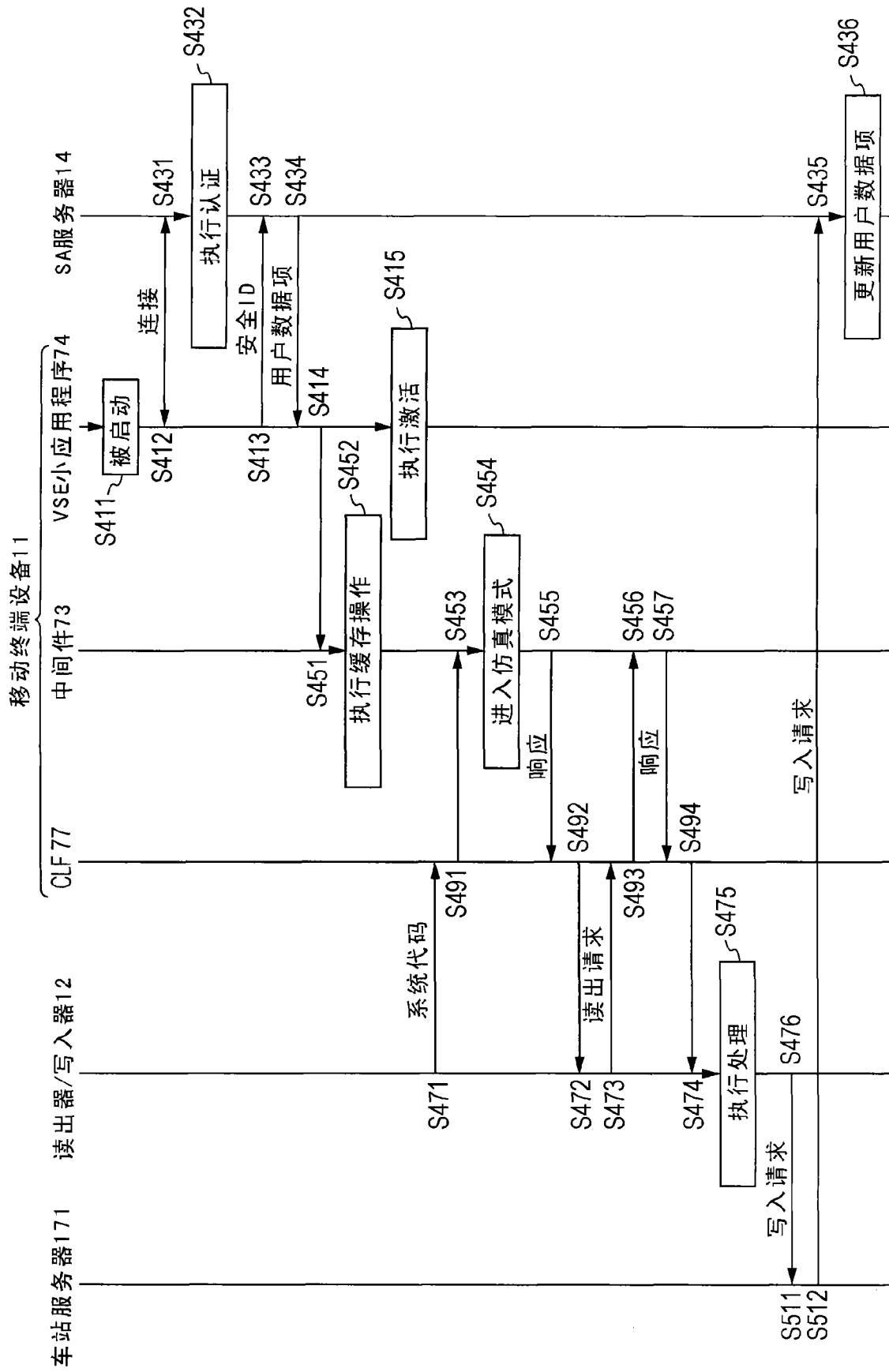


图 14