(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114218552 B
(45)授权公告日 2024.06.18

(21)申请号 202111351608.5

(22)申请日 2021.11.16

(65)同一申请的已公布的文献号
申请公布号 CN 114218552 A

(43)申请公布日 2022.03.22

(73)专利权人 成都智鑫易利科技有限公司
地址 610000 四川省成都市中国(四川)自由贸易试验区成都高新区天府大道中段500号1栋17楼1713号

(72)发明人 魏静 胡稼鑫 彭真 张军 邓廷胡佳

(74)专利代理机构 北京正华智诚专利代理事务所(普通合伙) 11870
专利代理师 杨浩林

(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/64(2013.01)
G06F 21/31(2013.01)

(56)对比文件

张靖宇;李志蜀;陈良银;邢建川;李宝林;李清.基于消息系统的可定制单点登出服务的设计与实现.四川大学学报(工程科学版).2007,(第05期),全文.

廖礼萍;鲍有文.基于跨域Cookie的单点登录系统的设计与实现.北京联合大学学报(自然科学版).2008,(第04期),全文.

审查员 冷凝

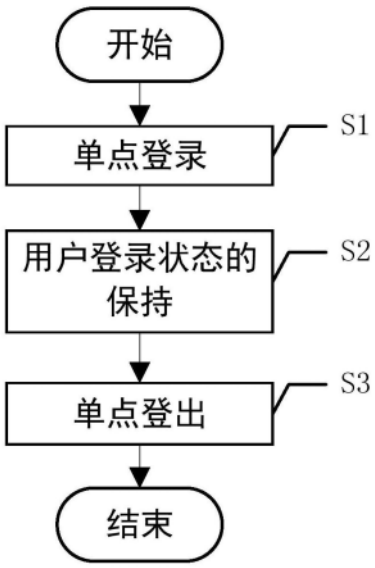
权利要求书2页 说明书5页 附图4页

(54)发明名称

一种采用服务总线实现超大用户量统一身份认证方法

(57)摘要

本发明公开了一种采用服务总线实现超大用户量统一身份认证方法,包括:S1、单点登录,S2、用户登录状态的保持;S3、单点登出;本发明通过这种分布式对用户身份的认证,实现超大量用户统一的身份认证方法;本发明解决了在超大用户量的情况下,所有用户在各个应用系统的所有操作都需要到认证中心验证用户的登录状态,这样认证中心的并发压力会很大,一般会采用增加硬件的方式解决,甚至于无法解决并发压力的问题,造成应用系统的响应速度慢的问题。



CN 114218552 B

1.一种采用服务总线实现超大用户量统一身份认证方法,其特征在于,包括以下步骤:

S1、单点登录:输入登录信息进行应用系统登录,将登录信息通过服务总线传输给认证中心,若登录信息正确,则根据用户登录状态反馈认证证书,应用系统登录成功,若登录信息错误,则认证无法通过,无法登录应用系统;

S2、用户登录状态的保持:当用户使用认证证书访问应用功能时,通过应用系统验证认证证书的有效性,若认证证书有效,则允许用户访问应用功能;若认证证书无效,则在认证中心本地验证认证证书或其他应用系统中验证认证证书,进一步判断认证证书是否有效,若认证证书有效,则将证书有效信息返回原应用系统,允许用户访问应用功能,若认证证书无效,则将证书登录超时信息返回原应用系统,原应用系统收到登录超时信息后提示用户登录超时并打开登录页面,用户认证应用系统过程结束;

所述步骤S2包括以下步骤:

S201、根据用户的登录信息,通过用户的认证证书访问应用系统的应用功能;

S202、通过应用系统在检索并判断本地是否存在该认证证书,若是,则跳转至步骤S203,若否,则将认证证书和证书验证请求通过服务总线传输至认证中心,并跳转至步骤S204;

S203、判断当前时间与应用系统的证书时间戳的差值是否小于系统阈值,若是,则未超时,允许用户使用应用功能,同时,将证书时间戳修改为当前时间,进入步骤S3,若否,则超时,将认证证书和证书验证请求通过服务总线传输至认证中心,并跳转至步骤S204;

S204、在认证中心接收到认证证书和证书验证请求后,根据用户的登录信息,在认证中心本地检索并判断是否存在该认证证书,若是,则跳转至步骤S205,若否,向应用系统返回证书登录超时信息,并跳转至步骤S213;

S205、判断当前时间与认证中心的证书时间戳的差值是否小于系统阈值,若是,则未超时,通过服务总线向原应用系统返回证书有效信息,并将认证中心的证书时间戳修改为当前时间,并跳转至步骤S214,若否,则超时,跳转至步骤S206;

S206、检索使用该认证证书的应用系统,判断是否存在除原应用系统外的其他使用该认证证书的应用系统,若是,则跳转步骤S207,若否,则向应用系统返回证书登录超时信息,并跳转至步骤S213;

S207、向服务总线发出证书验证请求、认证证书和应用系统编号;

S208、根据应用系统编号,将证书验证请求和认证证书发送给对应的应用系统;

S209、在其他使用该认证证书的应用系统收到证书验证请求后,检索并判断本地是否存在该认证证书,若是,则跳转至步骤S210,若否,则跳转至步骤S211;

S210、判断当前时间与本地的证书时间戳的差值是否小于系统阈值,若是,则未超时,将证书有效信息发送给服务总线,并将本地的证书时间戳修改为当前时间,并跳转至步骤S212,若否,则将证书失效信息发送至服务总线,并跳转至步骤S212;

S211、将证书失效信息发送至服务总线;

S212、通过认证中心收到所有证书失效信息和证书有效信息,判断是否除原应用系统外,认证证书在其他应用系统都失效,若是,则将认证证书在认证中心删除,并通过服务总线将登录超时信息传输至原应用系统,并跳转至步骤S213,若否,则通过服务总线将证书有效信息传输给原应用系统,并跳转至步骤S214;

S213、通过原应用系统收到登录超时信息后,提示该认证证书对应的用户登录超时,打开登录页面,将认证证书在本地的信息删除,用户认证应用系统过程结束;

S214、通过原应用系统收到证书有效信息后,将认证证书的证书时间戳修改为当前时间,允许用户使用应用功能,实现用户登录状态的保持,进入步骤S3;

S3、单点登出:在用户登出时,通过应用系统将用户登出信息发送到服务总线,并将本地的认证证书删除,通过服务总线转发用户登出信息到认证中心,认证中心接收到用户登出信息后,将用户登出信息发送给其它使用该认证证书的应用系统,并删除本地的该认证证书,用户认证应用系统过程结束。

2.根据权利要求1所述的采用服务总线实现超大用户量统一身份认证方法,其特征在于,所述步骤S1具体包括以下步骤:

S11、输入用户账户和密码的登录信息进行应用系统登录;

S12、通过应用系统获取登录信息,并通过服务总线将登录信息和应用系统编码传输给认证中心;

S13、通过认证中心判断登录信息是否正确,若是,则验证通过,并跳转至步骤S14,若否,则验证不通过,并将登录失败信息通过服务总线返回应用系统,通过应用系统提示登录失败并跳转到登录页面,用户认证应用系统过程结束;

S14、判断用户是否已处于已登录状态,若是,跳转至步骤S15,若否,则跳转至步骤S16;

S15、根据登录信息,检索用户的认证证书并通过服务总线返回认证证书,跳转至步骤S17;

S16、在认证中心生成并向服务总线返回认证证书,并保存登录信息、认证证书、证书时间戳和应用系统编号,跳转至步骤S17;

S17、在应用系统接收认证证书后,用户登录成功,并保存登录信息、认证证书和证书时间戳,进入步骤S2。

3.根据权利要求1所述的采用服务总线实现超大用户量统一身份认证方法,其特征在于,所述步骤S3具体包括以下步骤:

S31、在用户登出时,通过应用系统将用户登出信息发送给服务总线,并将本地认证证书删除;

S32、通过服务总线将用户登出信息转发至认证中心;

S33、根据用户登出信息对应的认证证书,检索并判断是否存在使用该认证证书的其他应用系统,若是,则删除认证中心的认证证书,并将用户登出信息通过服务总线转发至使用该认证证书的其他应用系统,并跳转至步骤S34,若否,则删除认证中心的认证证书,实现用户登出;

S34、在其他应用系统收到用户登出信息后,删除本地的对应的认证证书,实现用户登出。

4.根据权利要求1所述的采用服务总线实现超大用户量统一身份认证方法,其特征在于,所述服务总线采用的技术为Websocket。

一种采用服务总线实现超大用户量统一身份认证方法

技术领域

[0001] 本发明涉及,具体涉及一种采用服务总线实现超大用户量统一身份认证方法。

背景技术

[0002] 统一身份认证实现多应用系统的用户、角色和组织机构的统一化管理,实现各应用系统的单点登录、登录状态保持和单点登出等功能,是以统一身份认证服务为核心的服务使用模式,用户登录统一身份认证服务后,即可使用所有支持统一身份认证服务的应用系统。

[0003] 当前统一身份认证一般采用认证中心负责所有的单点登录、登录状态保持和单点登出的核心功能,在超大用户量的情况下,所有用户在各个应用系统的所有操作都需要到认证中心验证用户的登录状态,这样认证中心的并发压力会很大,一般会采用增加硬件的方式解决,甚至于无法解决并发压力的问题,造成应用系统的响应速度慢。

发明内容

[0004] 针对现有技术中的上述不足,本发明提供的一种采用服务总线实现超大用户量统一身份认证方法解决了在超大用户量的情况下,所有用户在各个应用系统的所有操作都需要到认证中心验证用户的登录状态,这样认证中心的并发压力会很大,一般会采用增加硬件的方式解决,甚至于无法解决并发压力的问题,造成应用系统的响应速度慢的问题。

[0005] 为了达到上述发明目的,本发明采用的技术方案为:一种采用服务总线实现超大用户量统一身份认证方法,包括以下步骤:

[0006] S1、单点登录:输入登录信息进行应用系统登录,应用将登录信息通过服务总线传输给认证中心,登录信息正确的,根据用户登录状态反馈认证证书,应用系统登录成功,登录信息错误的,无法登录应用系统;

[0007] S2、用户登录状态的保持:用户使用认证证书访问应用功能时,应用系统需验证认证证书的有效性,若认证证书有效,则允许用户访问应用功能;若认证证书无效,则在认证中心本地验证认证证书或其他应用系统中验证认证证书,进一步判断认证证书是否有效,若认证证书有效,则将证书有效信息返回原应用系统,允许用户访问应用功能,若认证证书无效,则将证书登录超时信息返回原应用系统,原应用系统收到登录超时信息后提示用户登录超时并打开登录页面,用户认证应用系统过程结束;

[0008] S3、单点登出:在用户登出时,应用系统将用户登出信息发送到服务总线,并将本地的认证证书删除,服务总线转发用户登出信息到认证中心,认证中心接收到用户登出信息后,将用户登出信息发送给其它使用该认证证书的应用系统,并删除本地的该认证证书,用户认证应用系统过程结束。

[0009] 进一步地,单点登录具体包括以下步骤:

[0010] S11、输入用户账户和密码的登录信息进行应用系统登录;

[0011] S12、通过应用系统获取登录信息,并通过服务总线将登录信息和应用系统编码传

输给认证中心；

[0012] S13、经认证中心判断登录信息是否正确，若是，则验证通过，并跳转至步骤S14，若否，则验证不通过，并将登录失败信息通过服务总线返回应用系统，应用系统提示登录失败并跳转到登录页面，用户认证应用系统过程结束；

[0013] S14、判断用户是否已处于已登录状态，若是，跳转至步骤S15，若否，则跳转至步骤S16；

[0014] S15、根据登录信息，检索用户的认证证书并通过服务总线返回认证证书，跳转至步骤S17；

[0015] S16、在认证中心生成并向服务总线返回认证证书，并保存登录信息、认证证书、证书时间戳和应用系统编号，跳转至步骤S17；

[0016] S17、在应用系统接收认证证书后，用户登录成功，并保存登录信息、认证证书和证书时间戳，进入步骤S2。

[0017] 进一步地，用户登录状态的保持具体包括以下步骤：

[0018] S201、根据用户的登录信息，通过用户的认证证书访问应用系统的应用功能；

[0019] S202、通过应用系统在检索并判断本地是否存在该认证证书，若是，则跳转至步骤S203，若否，则将认证证书和证书验证请求通过服务总线传输至认证中心，并跳转至步骤S204；

[0020] S203、判断当前时间与应用系统的证书时间戳的差值是否小于系统阈值，若是，则未超时，允许用户使用应用功能，同时，将证书时间戳修改为当前时间，进入步骤S3，若否，则超时，将认证证书和证书验证请求通过服务总线传输至认证中心，并跳转至步骤S204；

[0021] S204、在认证中心接收到认证证书和证书验证请求后，根据用户的登录信息，在认证中心本地检索并判断是否存在该认证证书，若是，则跳转至步骤S205，若否，向应用系统返回证书登录超时信息，并跳转至步骤S213；

[0022] S205、判断当前时间与认证中心的证书时间戳的差值是否小于系统阈值，若是，则未超时，通过服务总线向原应用系统返回证书有效信息，并将认证中心的证书时间戳修改为当前时间，并跳转至步骤S214，若否，则超时，跳转至步骤S206；

[0023] S206、检索使用该认证证书的应用系统，判断是否存在除原应用系统外的其他使用该认证证书的应用系统，若是，则跳转步骤S207，若否，则向应用系统返回证书登录超时信息，并跳转至步骤S213；

[0024] S207、向服务总线发出证书验证请求、认证证书和应用系统编号；

[0025] S208、根据应用系统编号，将证书验证请求和认证证书发送给对应的应用系统；

[0026] S209、在其他使用该认证证书的应用系统收到证书验证请求后，检索并判断本地是否存在该认证证书，若是，则跳转至步骤S210，若否，则跳转至步骤S211；

[0027] S210、判断当前时间与本地的证书时间戳的差值是否小于系统阈值，若是，则未超时，将证书有效信息发送给服务总线，并将本地的证书时间戳修改为当前时间，并跳转至步骤S212，若否，则将证书失效信息发送至服务总线，并跳转至步骤S212；

[0028] S211、将证书失效信息发送至服务总线；

[0029] S212、通过认证中心收到所有证书失效信息和证书有效信息，判断是否除原应用系统外，认证证书在其他应用系统都失效，若是，则将认证证书在认证中心删除，并通过服

务总线将登录超时信息传输至原应用系统,并跳转至步骤S213,若否,则通过服务总线将证书有效信息传输给原应用系统,并跳转至步骤S214;

[0030] S213、通过原应用系统收到登录超时信息后,提示该认证证书对应的用户登录超时,打开登录页面,将认证证书在本地的信息删除,用户认证应用系统过程结束;

[0031] S214、通过原应用系统收到证书有效信息后,将认证证书的证书时间戳修改为当前时间,允许用户使用应用功能,实现用户登录状态的保持。

[0032] 进一步地,单点登出具体包括以下步骤:

[0033] S31、在用户登出时,通过应用系统将用户登出信息发送给服务总线,并将本地认证证书删除;

[0034] S32、通过服务总线将用户登出信息转发至认证中心,;

[0035] S33、根据用户登出信息对应的认证证书,检索并判断是否存在使用该认证证书的其他应用系统,若是,则删除认证中心的认证证书,并将用户登出信息通过服务总线转发至使用该认证证书的其他应用系统,并跳转至步骤S34,若否,则删除认证中心的认证证书,实现用户登出;

[0036] S34、在其他应用系统收到用户登出信息后,删除本地的对应的认证证书,实现用户登出。

[0037] 进一步地,服务总线采用的技术为Websocket。

[0038] 综上,本发明的有益效果为:

[0039] (1)、本发明将用户分散到各应用系统,各用户在访问各应用系统的应用功能时,由各应用功能在本地对各用户进行验证,将验证未通过的,再送往认证中心验证,减少认证中心工作量,提高其响应速度;

[0040] (2)、将登录信息、认证证书和证书时间戳保存在各应用系统中,便于各应用系统对各用户进行验证时的数据调取。

[0041] (3)、在用户访问应用功能时,先在认证中心检索认证证书和判断超时情况,在认证中心认证通过时,不再将认证证书发送至其他应用系统进行验证,进一步减少其他系统的工作量,在认证中心认证不通过时,将认证证书发送至其他应用系统进行验证,利用其他应用系统本地保存的信息对其进行验证,各应用系统均能独立的对用户进行验证,实现用户登录状态的保持。

[0042] (4)、本发明通过这种分布式对用户身份的认证,实现超大量用户统一的身份认证方法。

附图说明

[0043] 图1为一种采用服务总线实现超大用户量统一身份认证方法的流程图

[0044] 图2为单点登录的流程图;

[0045] 图3为用户登录状态的保持的流程图;

[0046] 图4为单点登出的流程图。

具体实施方式

[0047] 下面对本发明的具体实施方式进行描述,以便于本技术领域的技术人员理解本发

明,但应该清楚,本发明不限于具体实施方式的范围,对本技术领域的普通技术人员来讲,只要各种变化在所附的权利要求限定和确定的本发明的精神和范围内,这些变化是显而易见的,一切利用本发明构思的发明创造均在保护之列。

[0048] 如图1所示,一种采用服务总线实现超大用户量统一身份认证方法,包括以下步骤:

[0049] S1、单点登录:输入登录信息进行应用系统登录,应用将登录信息通过服务总线传输给认证中心,登录信息正确的,根据用户登录状态反馈认证证书,应用系统登录成功,登录信息错误的,无法登录应用系统;

[0050] 如图2所示,单点登录具体包括以下步骤:

[0051] S11、输入用户账户和密码的登录信息进行应用系统登录;

[0052] S12、通过应用系统获取登录信息,并通过服务总线将登录信息和应用系统编码传输给认证中心;

[0053] S13、经认证中心判断登录信息是否正确,若是,则验证通过,并跳转至步骤S14,若否,则验证不通过,并将登录失败信息通过服务总线返回应用系统,应用系统提示登录失败并跳转到登录页面,用户认证应用系统过程结束;

[0054] S14、判断用户是否已处于已登录状态,若是,跳转至步骤S15,若否,则跳转至步骤S16;

[0055] S15、根据登录信息,检索用户的认证证书并通过服务总线返回认证证书,跳转至步骤S17;

[0056] S16、在认证中心生成并向服务总线返回认证证书,并保存登录信息、认证证书、证书时间戳和应用系统编号,跳转至步骤S17;

[0057] S17、在应用系统接收认证证书后,用户登录成功,并保存登录信息、认证证书和证书时间戳,进入步骤S2。

[0058] S2、用户登录状态的保持:用户使用认证证书访问应用功能时,应用系统需验证认证证书的有效性,若认证证书有效,则允许用户访问应用功能;若认证证书无效,则在认证中心本地验证认证证书或其他应用系统中验证认证证书,进一步判断认证证书是否有效,若认证证书有效,则将证书有效信息返回原应用系统,允许用户访问应用功能,若认证证书无效,则将证书登录超时信息返回原应用系统,原应用系统收到登录超时信息后提示用户登录超时并打开登录页面,用户认证应用系统过程结束;

[0059] 如图3所示,用户登录状态的保持具体包括以下步骤:

[0060] S201、根据用户的登录信息,通过用户的认证证书访问应用系统的应用功能;

[0061] S202、通过应用系统在检索并判断本地是否存在该认证证书,若是,则跳转至步骤S203,若否,则将认证证书和证书验证请求通过服务总线传输至认证中心,并跳转至步骤S204;

[0062] S203、判断当前时间与应用系统的证书时间戳的差值是否小于系统阈值,若是,则未超时,允许用户使用应用功能,同时,将证书时间戳修改为当前时间,进入步骤S3,若否,则超时,将认证证书和证书验证请求通过服务总线传输至认证中心,并跳转至步骤S204;

[0063] S204、在认证中心接收到认证证书和证书验证请求后,根据用户的登录信息,在认证中心本地检索并判断是否存在该认证证书,若是,则跳转至步骤S205,若否,向应用系统

返回证书登录超时信息,并跳转至步骤S213;

[0064] S205、判断当前时间与认证中心的证书时间戳的差值是否小于系统阈值,若是,则未超时,通过服务总线向原应用系统返回证书有效信息,并将认证中心的证书时间戳修改为当前时间,并跳转至步骤S214,若否,则超时,跳转至步骤S206;

[0065] S206、检索使用该认证证书的应用系统,判断是否存在除原应用系统外的其他使用该认证证书的应用系统,若是,则跳转步骤S207,若否,则向应用系统返回证书登录超时信息,并跳转至步骤S213;

[0066] S207、向服务总线发出证书验证请求、认证证书和应用系统编号;

[0067] S208、根据应用系统编号,将证书验证请求和认证证书发送给对应的应用系统;

[0068] S209、在其他使用该认证证书的应用系统收到证书验证请求后,检索并判断本地是否存在该认证证书,若是,则跳转至步骤S210,若否,则跳转至步骤S211;

[0069] S210、判断当前时间与本地的证书时间戳的差值是否小于系统阈值,若是,则未超时,将证书有效信息发送给服务总线,并将本地的证书时间戳修改为当前时间,并跳转至步骤S212,若否,则将证书失效信息发送至服务总线,并跳转至步骤S212;

[0070] S211、将证书失效信息发送至服务总线;

[0071] S212、通过认证中心收到所有证书失效信息和证书有效信息,判断是否除原应用系统外,认证证书在其他应用系统都失效,若是,则将认证证书在认证中心删除,并通过服务总线将登录超时信息传输至原应用系统,并跳转至步骤S213,若否,则通过服务总线将证书有效信息传输给原应用系统,并跳转至步骤S214;

[0072] S213、通过原应用系统收到登录超时信息后,提示该认证证书对应的用户登录超时,打开登录页面,将认证证书在本地的信息删除,用户认证应用系统过程结束;

[0073] S214、通过原应用系统收到证书有效信息后,将认证证书的证书时间戳修改为当前时间,允许用户使用应用功能,实现用户登录状态的保持。

[0074] S3、单点登出:在用户登出时,应用系统将用户登出信息发送到服务总线,并将本地的认证证书删除,服务总线转发用户登出信息到认证中心,认证中心接收到用户登出信息后,将用户登出信息发送给其它使用该认证证书的应用系统,并删除本地的该认证证书,用户认证应用系统过程结束。

[0075] 如图4所示,单点登出具体包括以下步骤:

[0076] S31、在用户登出时,通过应用系统将用户登出信息发送给服务总线,并将本地认证证书删除;

[0077] S32、通过服务总线将用户登出信息转发至认证中心,;

[0078] S33、根据用户登出信息对应的认证证书,检索并判断是否存在使用该认证证书的其他应用系统,若是,则删除认证中心的认证证书,并将用户登出信息通过服务总线转发至使用该认证证书的其他应用系统,并跳转至步骤S34,若否,则删除认证中心的认证证书,实现用户登出;

[0079] S34、在其他应用系统收到用户登出信息后,删除本地的对应的认证证书,实现用户登出。

[0080] 服务总线采用的技术为Websocket。

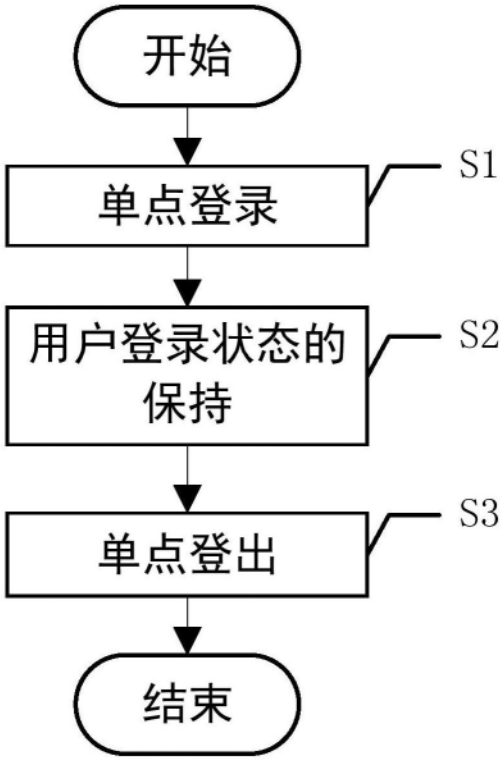


图1

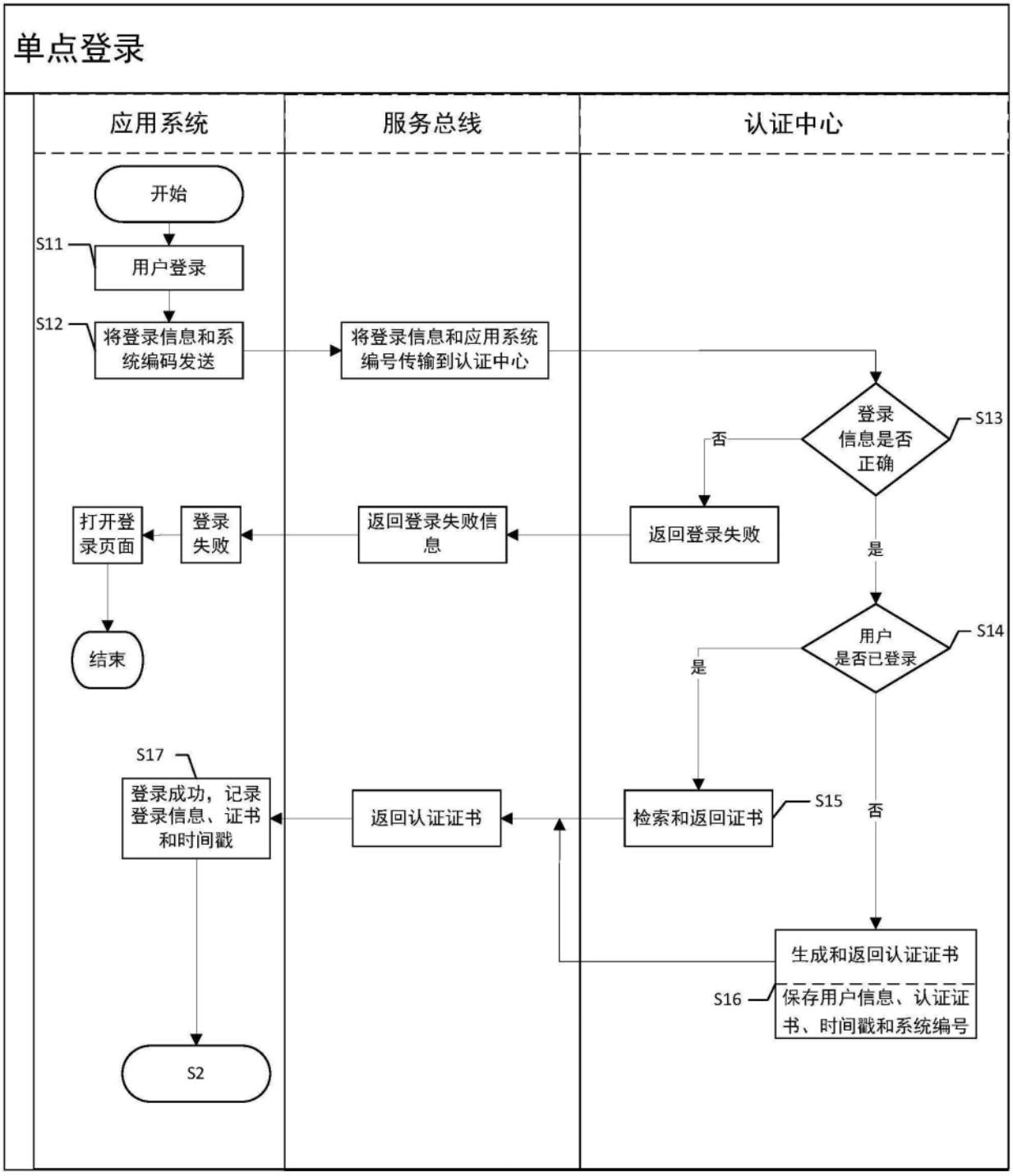

单点登录
应用系统
服务总线
认证中心
开始
S11
用户登录
S12
将登录信息和系统编码发送
将登录信息和应用系统编号传输到认证中心
登录信息是否正确
S13
否
是
返回登录失败
返回登录失败信息
登录失败
打开登录页面
结束
用户是否已登录
S14
是
否
检索和返回证书
S15
返回认证证书
S17
登录成功，记录登录信息、证书和时间戳
生成和返回认证证书
S16
保存用户信息、认证证书、时间戳和系统编号
S2

图2

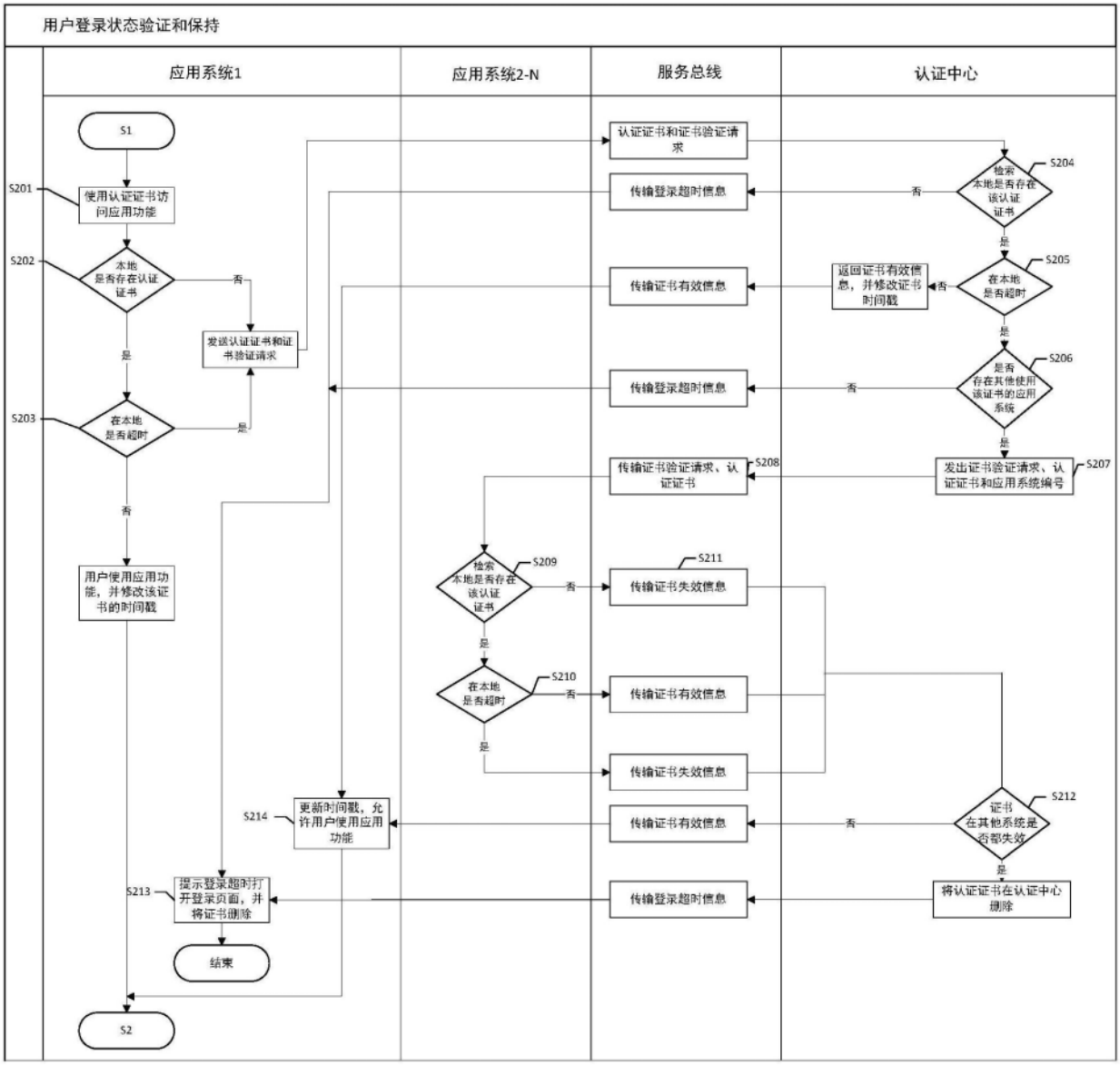

用户登录状态验证和保持
应用系统1
应用系统2-N
服务总线
认证中心
S1
S201
使用认证证书访问应用功能
S202
本地是否存在认证证书
否
是
发送认证证书和证书验证请求
S203
在本地是否超时
是
否
用户使用应用功能，并修改该证书的时间戳
S2
认证证书和证书验证请求
传输登录超时信息
传输证书有效信息
传输登录超时信息
传输证书验证请求、认证证书
S208
传输证书失效信息
传输证书有效信息
传输证书失效信息
传输证书有效信息
传输登录超时信息
S204
检索本地是否存在该认证证书
否
是
S205
在本地是否超时
返回证书有效信息，并修改证书时间戳
否
是
S206
是否存在其他使用该证书的应用系统
否
是
S207
发出证书验证请求、认证证书和应用系统编号
S209
检索本地是否存在该认证证书
否
是
S210
在本地是否超时
否
是
S211
S212
证书在其他系统是否都失效
否
是
将认证证书在认证中心删除
S214
更新时间戳，允许用户使用应用功能
S213
提示登录超时打开登录页面，并将证书删除
结束

图3

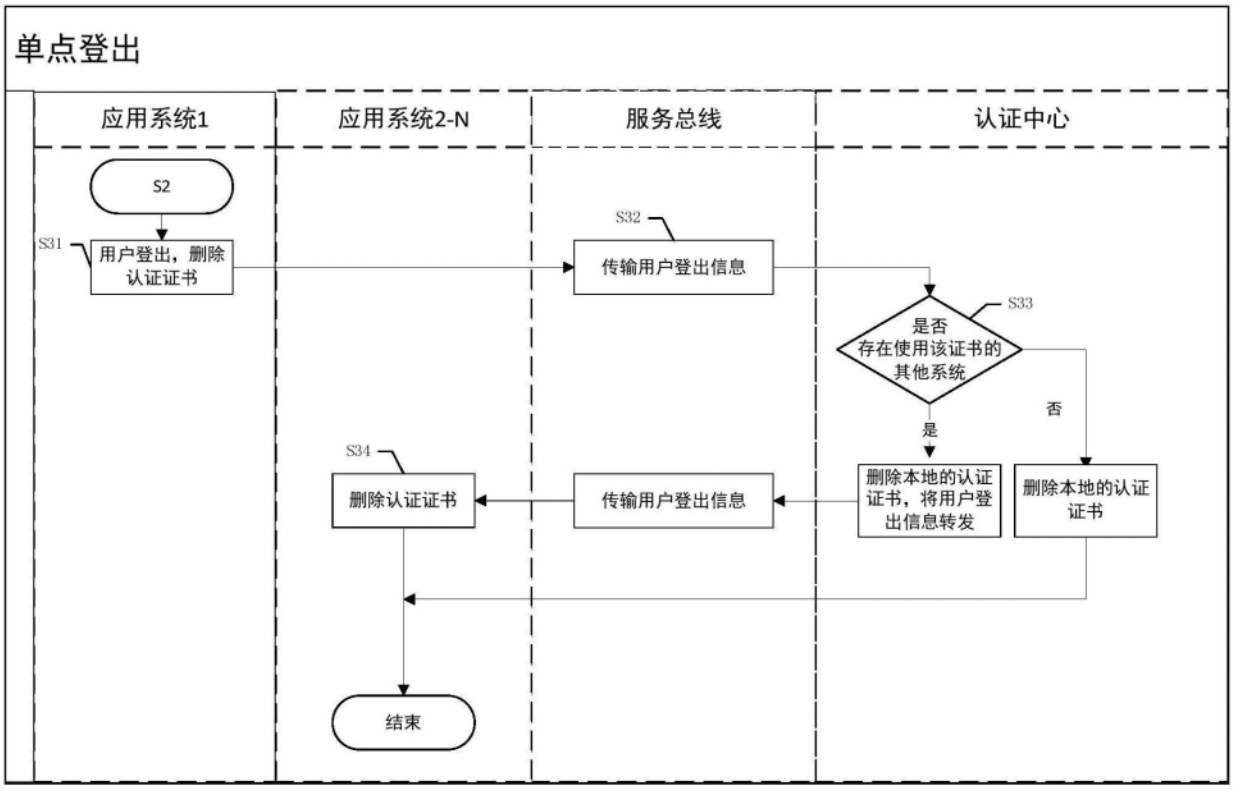

单点登出
应用系统1
应用系统2-N
服务总线
认证中心
S2
S31
用户登出，删除认证证书
S32
传输用户登出信息
S33
是否存在使用该证书的其他系统
是
否
S34
删除认证证书
传输用户登出信息
删除本地的认证证书，将用户登出信息转发
删除本地的认证证书
结束

图4