(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 107846281 B
(45)授权公告日 2020.12.08

(21)申请号 201711036923.2

(22)申请日 2017.10.30

(65)同一申请的已公布的文献号
申请公布号 CN 107846281 A

(43)申请公布日 2018.03.27

(73)专利权人 上海应用技术大学
地址 200235 上海市徐汇区漕宝路120-121号

(72)发明人 薛庆水 李文举 陈颖 舒明磊 杨瑞君 王栋 戴酉

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 田晓杰 胡晶

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 1503932 A,2004.06.09
CN 104160653 A,2014.11.19
WO 2017027134 A8,2017.09.28
US 2005022102 A1,2005.01.27
Qingshui Xue.Proxy Multi-Signature Binding Positioning Protocol.《2014 IEEE/CIC International Conference on Communications in China (ICCC)》.2015,第I节-第IV节,图1-2.

审查员 孙铭君

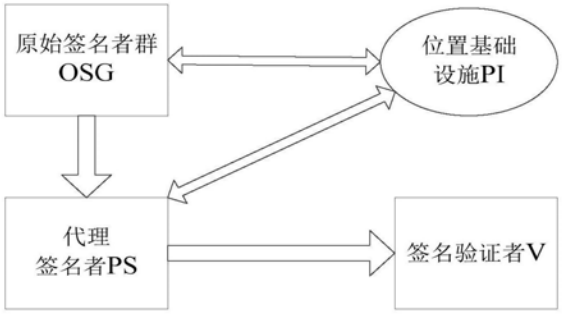
权利要求书2页 说明书6页 附图2页

(54)发明名称

基于位置的代理多重签名方法和系统

(57)摘要

本发明提供了一种基于位置的代理多重签名方法和系统,该方法包括:进行代理签名者PS、原始签名者群OSG以及位置基础设施PI的初始化;在PI的参与下完成原始签名者群OSG所在位置的真实性验证,然后通过PI来验证代理签名者PS的位置的真实性的认证,最后原始签名者群OSG完成对代理签名者PS的指定位置代理签名授权;代理签名者PS在PI的支持下完成其自己位置的认证功能,然后再执行对特定信息的代理签名功能;由代理签名验证者V来完成验证代理签名确实由指定位置的原始签名者群联合授权指定位置的代理签名者对预设信息进行了代理签名。本发明中的方法安全性高、应用范围广,实现了身份与位置的认证权力的转移。



CN 107846281 B

1.一种基于位置的代理多重签名方法,其特征在于,包括:

位置基础实施PI在初始化过程中获取安全参数1^k、主密钥mk、公开参数pp,并分别向原始签名者群OSG中的每个原始签名者OS发送唯一对应的身份信息;其中,假设原始签名者群OSG中包含有n个原始签名者OS,第i个原始签名者记为OS_i,其中i=1,2,3,…,n;则第i个原始签名者OS_i对应的身份信息为ID_i,n表示原始签名者的总数;

接收来自原始签名者OS_i发送的代理签名请求信息,所述代理签名请求信息中包含有该原始签名者OS_i对应的位置信息Pos_{OS_i};

通过位置定位协议确定每一个原始签名者OS_i对应的位置信息Pos_{OS_i}为有效信息时,向每一个原始签名者OS_i发送对应的确认信息;并生成代理授权密钥包$pdkp_{OS_i}$,i=1,2,3,…,n;$pdkp_{OS_i}$表示第i个原始签名者对应的代理授权密钥包;

向每个原始签名者发送对应的代理授权密钥包$pdkp_{OS_i}$;

接收检查者侧发送的代理授权证书dw,dw中包含有所有原始签名者和代理签名者的身份、位置、可签名消息类型、有效期信息;

根据所述代理授权证书dw生成代理签名密钥包pskp,并发送给代理签名者PS;其中,所述代理签名密钥包pskp是代理签名者在指定的位置时生成的,所述检查者为原始签名者群OSG中指定的任一个原始签名者。

2.根据权利要求1所述的基于位置的代理多重签名方法,其特征在于,所述代理授权密钥包中封装有位置定位协议、授权密钥、对应原始签名者的身份信息、代理签名者的身份信息、对应原始签名者的位置信息以及代理签名者的位置信息;

所述代理签名密钥包pskp中封装有位置定位协议、代理签名密钥、代理签名者的身份信息、代理签名者的位置信息、签名算法。

3.根据权利要求1或2所述的基于位置的代理多重签名方法,其特征在于,所述位置定位协议包括:全球定位系统GPS协议,用于确定原始签名者、代理签名者的位置。

4.一种基于位置的代理多重签名方法,其特征在于,包括:

原始签名者OS_i向位置基础实施PI发送代理签名请求信息,所述代理签名请求信息中包含有该原始签名者OS_i对应的位置信息Pos_{OS_i};其中,OS_i表示第i个原始签名者,Pos_{OS_i}表示第i个原始签名者对应的位置信息,其中i=1,2,3,…,n,n表示原始签名者的总数;

原始签名者OS_i接收位置基础实施PI发送的代理授权密钥包$pdkp_{OS_i}$,$i=1,2,3,\ldots,n$;$pdkp_{OS_i}$表示第i个原始签名者对应的代理授权密钥包;

根据代理授权密钥包$pdkp_{OS_i}$,确定原始签名者OS_i的位置有效时,生成相应的代理授权信息;所述代理授权信息中包含有原始签名者的身份信息、原始签名者的位置信息以及根据所述代理授权密钥包生成的签名dw_i,dw_i表示第i个代理授权密钥包$pdkp_{OS_i}$生成的签名;其中,所述代理签名密钥包pskp是代理签名者在指定的位置时生成的;

将所述代理授权信息发送给检查者,其中,所述检查者为原始签名者群OSG中指定的任一个原始签名者。

5.根据权利要求4所述的基于位置的代理多重签名方法,其特征在于,代理授权密钥包中封装有位置定位协议、授权密钥、对应原始签名者的身份信息、代理签名者的身份信息、

对应原始签名者的位置信息以及代理签名者的位置信息。

6.根据权利要求4或5所述的基于位置的代理多重签名方法，其特征在于，当原始签名者作为检查者时，还包括：

确定原始签名者群OSG中指定的任一个原始签名者作为检查者，所述检查者检查代理授权密钥包$pdkp_{OS_i}$生成的签名dw_i是否由原始签名者OS_i来生成，

若否，则无效，结束流程；

若是，

则dw_i有效，判断所有的dw_i是否全部有效，i＝1,2,3,…,n，若全部有效，则生成代理授权证书，令$dw=\prod_{i=1}^{n} dw_i$，dw表示代理授权证书，dw中包含有所有原始签名者和代理签名者的身份信息、位置信息、可签名消息类型信息、有效期信息；

向代理签名者PS发送代理授权证书。

7.一种基于位置的代理多重签名方法，其特征在于，包括：

接收位置基础实施PI发送的代理签名密钥包pskp和检查者发送的代理授权证书；其中，所述代理签名密钥包pskp是代理签名者在指定的位置时生成的，所述检查者为原始签名者群OSG中指定的任一个原始签名者；

根据代理签名密钥包pskp中封装的位置定位协议确定代理签名者PS自身的位置信息Pos_{PS}是否有效，若无效，则结束流程；

若有效，

则向签名验证者V发送多重签名，所述多重签名记为：(m,s,dw,pp)，(m,s,dw,pp)表示针对消息m的签名s，且签名s的有效次数为1次；

其中，位置信息Pos_{PS}有效是指：代理签名者PS的位置信息与代理授权证书中关于代理签名者PS的位置信息一致。

8.一种基于位置的代理多重签名系统，其特征在于，包括：位置基础设施PI、原始签名者OS、代理签名者PS以及签名验证者V；其中，

所述位置基础设施PI用于执行权利要求1-3中任一项所述的基于位置的代理多重签名方法；

所述原始签名者OS用于执行权利要求4-6中任一项所述的基于位置的代理多重签名方法；

所述代理签名者PS用于执行权利要求7所述的基于位置的代理多重签名方法；

所述签名验证者V用于接收代理签名者PS发送的代理多重签名(m,s,dw,pp)；其中，(m,s,dw,pp)表示针对消息m的签名s，且签名s的有效次数为1次；

通过原始签名者的身份信息和位置信息、代理签名者的身份信息和位置信息、公开参数pp来检查代理授权证书是否有效，若无效，则结束流程；

若有效，则通过预设的多重签名验证算法来验证s是否是消息m的代理多重签名，若验证成功，则确认消息m确实由代理签名者在指定的位置Pos_{PS}代表原始签名者群。

基于位置的代理多重签名方法和系统

技术领域

[0001] 本发明涉及网络信息安全技术领域，具体地，涉及基于位置的代理多重签名方法和系统。

背景技术

[0002] 近年来，基于位置的相关服务与应用以及代理签名技术都得到了深入的研究与发展。基于位置的服务与应用能够为用户的位置实施定位，也可以为用户提供与位置相关的服务，比如旅馆服务、餐饮服务、邮政服务以及旅游服务等。代理签名技术则提供了一个用户授权另一个用户实施代理签名的能力，进而实现对消息的完整性、不可否认性以及来源进行鉴别的功能。

[0003] 但是，现有技术还无法在移动互联网环境下，实现由位于不同位置的用户群联合向处于另一位置的单一用户授权代表用户群在指定的位置实施代理签名的功能。因此，无法保证用户位置安全以及与位置相关的消息完整性、认证性以及不可否认性。

发明内容

[0004] 针对现有技术中的缺陷，本发明的目的是提供一种基于位置的代理多重签名方法和系统。

[0005] 第一方面，本发明提供一种基于位置的代理多重签名方法，包括：

[0006] 位置基础实施PI在初始化过程中获取安全参数1^k、主密钥mk、公开参数pp，并分别向原始签名者群OSG中的每个原始签名者OS发送唯一对应的身份信息；其中，假设原始签名者群OSG中包含有n个原始签名者OS，第i个原始签名者记为OS_i，其中i＝1,2,3,…,n；则第i个原始签名者OS_i对应的身份信息为ID_i，n表示原始签名者的总数；

[0007] 接收来自原始签名者OS_i发送的代理签名请求信息，所述代理签名请求信息中包含有该原始签名者OS_i对应的位置信息Pos_{OS_i}；

[0008] 通过位置定位协议确定每一个原始签名者OS_i对应的位置信息Pos_{OS_i}为有效信息时，向每一个原始签名者OS_i发送对应的确认信息；并生成代理授权密钥包$pdkp_{OS_i}$，i＝1,2,3,…,n；$pdkp_{OS_i}$表示第i个原始签名者对应的代理授权密钥包；

[0009] 向每个原始签名者发送对应的代理授权密钥包$pdkp_{OS_i}$；

[0010] 接收检查者侧发送的代理授权证书dw，dw中包含有所有原始签名者和代理签名者的身份、位置、可签名消息类型、有效期信息；

[0011] 根据所述代理授权证书dw生成代理签名密钥包pskp，并发送给代理签名者PS。

[0012] 可选地，所述代理授权密钥包中封装有位置定位协议、授权密钥、对应原始签名者的身份信息、代理签名者的身份信息、对应原始签名者的位置信息以及代理签名者的位置信息；

[0013] 所述代理签名密钥包pskp中封装有位置定位协议、代理签名密钥、代理签名者的

身份信息、代理签名者的位置信息、签名算法。

[0014] 可选地，所述位置定位协议包括：全球定位系统GPS协议，用于确定原始签名者、代理签名者的位置。

[0015] 第二方面，本发明提供一种基于位置的代理多重签名方法，包括：

[0016] 原始签名者OS_i向位置基础实施PI发送代理签名请求信息，所述代理签名请求信息中包含有该原始签名者OS_i对应的位置信息Pos_{OS_i}；其中，OS_i表示第i个原始签名者，Pos_{OS_i}表示第i个原始签名者对应的位置信息，其中i＝1,2,3,…,n,n表示原始签名者的总数；

[0017] 原始签名者OS_i接收位置基础实施PI发送的代理授权密钥包$pdkp_{OS_i}$，i＝1,2,3,…,n；$pdkp_{OS_i}$表示第i个原始签名者对应的代理授权密钥包；

[0018] 根据代理授权密钥包$pdkp_{OS_i}$，确定原始签名者OS_i的位置有效时，生成相应的代理授权信息；所述代理授权信息中包含有原始签名者的身份信息、原始签名者的位置信息以及根据所述代理授权密钥包生成的签名dw_i，dw_i表示第i个代理授权密钥包$pdkp_{OS_i}$生成的签名；

[0019] 将所述代理授权信息发送给检查者，其中，所述检查者为原始签名者群OSG中指定的任一个原始签名者。

[0020] 可选地，代理授权密钥包中封装有位置定位协议、授权密钥、对应原始签名者的身份信息、代理签名者的身份信息、对应原始签名者的位置信息以及代理签名者的位置信息；

[0021] 可选地，当原始签名者作为检查者时，还包括：

[0022] 确定原始签名者群OSG中指定的任一个原始签名者作为检查者，所述检查者检查代理授权密钥包$pdkp_{OS_i}$生成的签名dw_i是否由原始签名者OS_i来生成，

[0023] 若否，则无效，结束流程；

[0024] 若是，

[0025] 则dw_i有效，判断所有的dw_i是否全部有效，i＝1,2,3,…,n，若全部有效，则生成代理授权证书，令$dw=\prod_{i=1}^{n} dw_i$，dw表示代理授权证书，dw中包含有所有原始签名者和代理签名者的身份信息、位置信息、可签名消息类型信息、有效期信息；

[0026] 向代理签名者PS发送代理授权证书。

[0027] 第三方面，本发明提供一种基于位置的代理多重签名方法，包括：

[0028] 接收位置基础实施PI发送的代理签名密钥包pskp和检查者发送的代理授权证书；

[0029] 根据代理签名密钥包pskp中封装的位置定位协议确定代理签名者PS自身的位置信息Pos_{PS}是否有效，若无效，则结束流程；

[0030] 若有效，

[0031] 则向签名验证者V发送多重签名，所述多重签名记为：(m,s,dw,pp)，(m,s,dw,pp)表示针对消息m的签名s，且签名s的有效次数为1次；

[0032] 其中，位置信息Pos_{PS}有效是指：代理签名者PS的位置信息与代理授权证书中关于代理签名者PS的位置信息一致。

[0033] 第四方面，本发明提供一种基于位置的代理多重签名方法，包括：

[0034] 接收代理签名者PS发送的代理多重签名(m,s,dw,pp)；其中，(m,s,dw,pp)表示针

对消息m的签名s，且签名s的有效次数为1次；

[0035] 通过原始签名者的身份信息和位置信息、代理签名者的身份信息和位置信息、公开参数pp来检查代理授权证书是否有效，若无效，则结束流程；

[0036] 若有效，则通过预设的多重签名验证算法来验证s是否是消息m的代理多重签名，若验证成功，则确认消息m确实由代理签名者在指定的位置Pos_{PS}代表原始签名者群。

[0037] 第五方面，本发明提供一种基于位置的代理多重签名系统，包括：位置基础设施PI、原始签名者OS、代理签名者PS以及签名验证者V；其中，

[0038] 所述位置基础设施PI用于执行权利要求第一方面中任一项所述的基于位置的代理多重签名方法；

[0039] 所述原始签名者OS用于执行权利要求第二方面中任一项所述的基于位置的代理多重签名方法；

[0040] 所述代理签名者PS用于执行权利要求第三方面所述的基于位置的代理多重签名方法；

[0041] 所述签名验证者V用于执行权利要求第四方面所述的基于位置的代理多重签名方法。

[0042] 与现有技术相比，本发明具有如下的有益效果：

[0043] 本发明提供的能够实现处于不同位置的多名用户授权处于指定位置的用户代表多名用户进行签名的功能，并确保了基于位置的消息的完整性和不可否认性，使得与位置相关的信息更加安全可靠。进一步地，在可选方案中，本发明提供的基于位置的代理多重签名方法，还对代理签名者发布的签名消息进行验证，且不限定代理签名验证者的位置，进一步保证了签名消息的可靠性和安全性。

附图说明

[0044] 通过阅读参照以下附图对非限制性实施例所作的详细描述，本发明的其它特征、目的和优点将会变得更明显：

[0045] 图1为本发明中方法的应用场景示意图；

[0046] 图2为本发明一实施例提供的基于位置的代理多重签名方法的流程图；

[0047] 图3为本发明一实施例中代理授权密钥包的流程示意图；

[0048] 图4为本发明一实施例中代理签名密钥包的流程示意图。

具体实施方式

[0049] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明，但不以任何形式限制本发明。应当指出的是，对本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变化和改进。这些都属于本发明的保护范围。

[0050] 应用本发明提供的基于位置的代理多重签名方法的系统包括：位置基础设施(Position Infrastructure,PI)、原始签名者(Original Signer,OS)、代理签名者(Proxy Signer,PS)以及签名验证者(Verifier,V)；其中，所有原始签名者构成原始签名者群(Original Signer Group,OSG)。如图1所示，原始签名者群OSG联合授权代理签名者PS，在

位置基础设施PI的协助之下，完成对指定位置的代理签名者PS对特定信息的代理签名能力。

[0051] 如图2所示，根据本发明提供的基于位置的代理多重签名方法，可以包括：第一步：进行代理签名者PS、原始签名者群OSG以及位置基础设施PI的初始化；第二步：首先在PI的参与下完成原始签名者群OSG所在位置的真实性验证，然后PI来验证代理签名者PS的位置的真实性的认证，最后原始签名者群OSG完成对代理签名者PS的指定位置代理签名授权；第三步：首先代理签名者PS要在PI的支持下完成其自己位置的认证功能，然后再执行对特定信息的代理签名功能；第四步：由代理签名验证者V来完成验证代理签名确实由指定位置的原始签名者群联合授权指定位置的代理签名者对预设信息进行了代理签名。

[0052] 进一步地，如图3所示，原始签名者OS(原始签名者群OSG)首先在PI的协助下来判断对应的原始签名者OS是否在指定的位置，如是则生成代理授权密钥；若否，结束。其中，代理授权密钥作为代理授权生成模块的输入，并结合授权证书信息，生成代理授权证书，发送给代理签名者PS。

[0053] 进一步地，如图4所示，代理签名者PS首先在PI的协助下来判断是否在指定的位置，如是则生成代理签名密钥，若否，则结束。其中，代理签名密钥作为代理签名生成的输入，外加待签名消息，生成代理签名，发送给代理签名验证者V。

[0054] 本发明提供的基于位置的代理多重签名方法，能够实现处于不同位置的多名用户授权处于指定位置的用户代表多名用户进行签名的功能，并确保了基于位置的消息的完整性和不可否认性，使得与位置相关的信息更加安全可靠。

[0055] 可选地，本发明提供的基于位置的代理多重签名方法，还对代理签名者发布的签名消息进行验证，且不限定代理签名验证者的位置，进一步保证了签名消息的可靠性和安全性。

[0056] 本发明中的方法与传统基于身份验证的方法不同，实现了基于身份与位置的认证权利的转移，满足移动互联网环境下，多名不同位置的用户群对任意指定用于授权实施代理签名的安全性要求。

[0057] 为了更加清楚地描述本发明中的方法，下面结合具体实施例进行详细的说明。具体地，位置基础设置PI侧包括如下步骤：

[0058] 步骤A1：位置基础实施PI在初始化过程中获取安全参数1^k、主密钥mk、公开参数pp，并分别向原始签名者群OSG中的每个原始签名者OS发送唯一对应的身份信息；其中，假设原始签名者群OSG中包含有n个原始签名者OS，第i个原始签名者记为OS_i，其中i＝1,2,3,…,n；则第i个原始签名者OS_i对应的身份信息为ID_i；

[0059] 步骤A2：接收来自原始签名者OS_i发送的代理签名请求信息，所述代理签名请求信息中包含有该原始签名者OS_i对应的位置信息Pos_{OS_i}；

[0060] 步骤A3：通过位置定位协议确定每一个原始签名者OS_i对应的位置信息Pos_{OS_i}为有效信息时，向每一个原始签名者OS_i发送对应的确认信息；并生成代理授权密钥包$pdkp_{OS_i}$，i＝1,2,3,…,n；$pdkp_{OS_i}$表示第i个原始签名者对应的代理授权密钥包；其中，所述代理授权密钥包中封装有位置定位协议、授权密钥、对应原始签名者的身份信息、代理签名者的身份信息、对应原始签名者的位置信息以及代理签名者的位置信息；

[0061] 步骤A4:向每个原始签名者发送对应的代理授权密钥包 $pdkp_{OS_i}$;

[0062] 步骤A5:接收检查者侧发送的代理授权证书dw,dw中包含有所有原始签名者和代理签名者的身份、位置、可签名消息类型、有效期信息;

[0063] 步骤A6:根据所述代理授权证书dw生成代理签名密钥包pskp,并发送给代理签名者PS,其中,所述代理签名密钥包pskp中封装有位置定位协议、代理签名密钥、代理签名者的身份信息、代理签名者的位置信息、签名算法等。

[0064] 原始签名者OS侧(原始签名者群OSG侧)包括如下步骤:

[0065] 步骤B1:原始签名者OS_i向位置基础实施PI发送代理签名请求信息,所述代理签名请求信息中包含有该原始签名者OS_i对应的位置信息 Pos_{OS_i} ;其中,OS_i表示第i个原始签名者, Pos_{OS_i} 表示第i个原始签名者对应的位置信息,其中i=1,2,3,…,n,n表示原始签名者的总数;

[0066] 步骤B2:原始签名者OS_i接收位置基础实施PI发送的代理授权密钥包 $pdkp_{OS_i}$,i=1,2,3,…,n; $pdkp_{OS_i}$ 表示第i个原始签名者对应的代理授权密钥包;其中,代理授权密钥包中封装有位置定位协议、授权密钥、对应原始签名者的身份信息、代理签名者的身份信息、对应原始签名者的位置信息以及代理签名者的位置信息;

[0067] 步骤B3:根据代理授权密钥包 $pdkp_{OS_i}$,确定原始签名者OS_i的位置有效时,生成相应的代理授权信息;所述代理授权信息中包含有原始签名者的身份信息、原始签名者的位置信息以及根据所述代理授权密钥包生成的签名dw_i,dw_i表示第i个代理授权密钥包 $pdkp_{OS_i}$ 生成的签名;

[0068] 步骤B4:将所述代理授权信息发送给检查者(Clerk),其中,所述检查者为原始签名者群OSG中指定的任一个原始签名者。

[0069] 检查者侧,包括如下步骤:

[0070] 步骤C1:确定原始签名者群OSG中指定的任一个原始签名者作为检查者,所述检查者检查代理授权密钥包 $pdkp_{OS_i}$ 生成的签名dw_i是否由原始签名者OS_i来生成,若是,则dw_i有效,执行步骤C2,若否,则无效,结束流程;

[0071] 步骤C2:判断所有的dw_i是否全部有效,i=1,2,3,…,n,若全部有效,则生成代理授权证书,令 $dw=\prod_{i=1}^{n} dw_i$,dw表示代理授权证书,dw中包含有所有原始签名者和代理签名者的身份信息、位置信息、可签名消息类型信息、有效期信息;

[0072] 步骤C3:向代理签名者PS发送代理授权证书。

[0073] 代理签名者PS侧,包括如下步骤:

[0074] 步骤D1:接收位置基础实施PI发送的代理签名密钥包pskp和检查者发送的代理授权证书;

[0075] 步骤D2:根据代理签名密钥包pskp中封装的位置定位协议确定代理签名者PS自身的位置信息Pos_{PS}是否有效,若有效,则执行步骤D3;若无效,则结束流程;其中,位置信息Pos_{PS}有效是指:代理签名者PS的位置信息与代理授权证书中关于代理签名者PS的位置信息一致;

[0076] 步骤D3:向签名验证者V发送多重签名,所述多重签名记为:(m,s,dw,pp),(m,s,dw,pp)表示针对消息m的签名s,且签名s的有效次数为1次。

[0077] 签名验证者V侧,包括如下步骤:

[0078] 步骤E1:接收代理签名者PS发送的代理多重签名(m,s,dw,pp);

[0079] 步骤E2:通过原始签名者的身份信息和位置信息、代理签名者的身份信息和位置信息、公开参数pp来检查代理授权证书是否有效,若有效,则执行步骤E3,若无效,则结束流程;

[0080] 步骤E3:通过预设的多重签名验证算法来验证s是否是消息m的代理多重签名,若验证成功,则确认消息m确实由代理签名者在指定的位置Pos_{PS}代表原始签名者群(在位置Pos_{OS_i}(i=1,2,...,n))进行的签名;若验证失败,则结束流程。

[0081] 需要说明的是,本发明提供的所述基于位置的代理多重签名方法中的步骤,可以利用所述基于位置的代理多重签名系统中对应的模块、装置、单元等予以实现,本领域技术人员可以参照所述系统的技术方案实现所述方法的步骤流程,即,所述系统中的实施例可理解为实现所述方法的优选例,在此不予赘述。

[0082] 本领域技术人员知道,除了以纯计算机可读程序代码方式实现本发明提供的系统及其各个装置以外,完全可以通过将方法步骤进行逻辑编程来使得本发明提供的系统及其各个装置以逻辑门、开关、专用集成电路、可编程逻辑控制器以及嵌入式微控制器等的形式来实现相同功能。所以,本发明提供的系统及其各项装置可以被认为是一种硬件部件,而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构;也可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0083] 以上对本发明的具体实施例进行了描述。需要理解的是,本发明并不局限于上述特定实施方式,本领域技术人员可以在权利要求的范围内做出各种变化或修改,这并不影响本发明的实质内容。在不冲突的情况下,本申请的实施例和实施例中的特征可以任意相互组合。

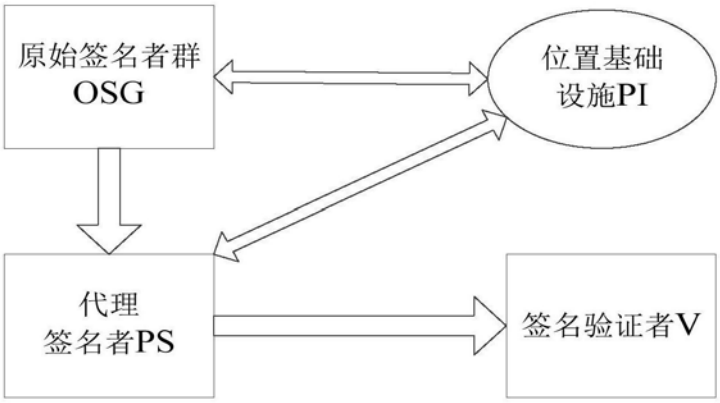

原始签名者群
OSG
位置基础
设施PI
代理
签名者PS
签名验证者V

图1

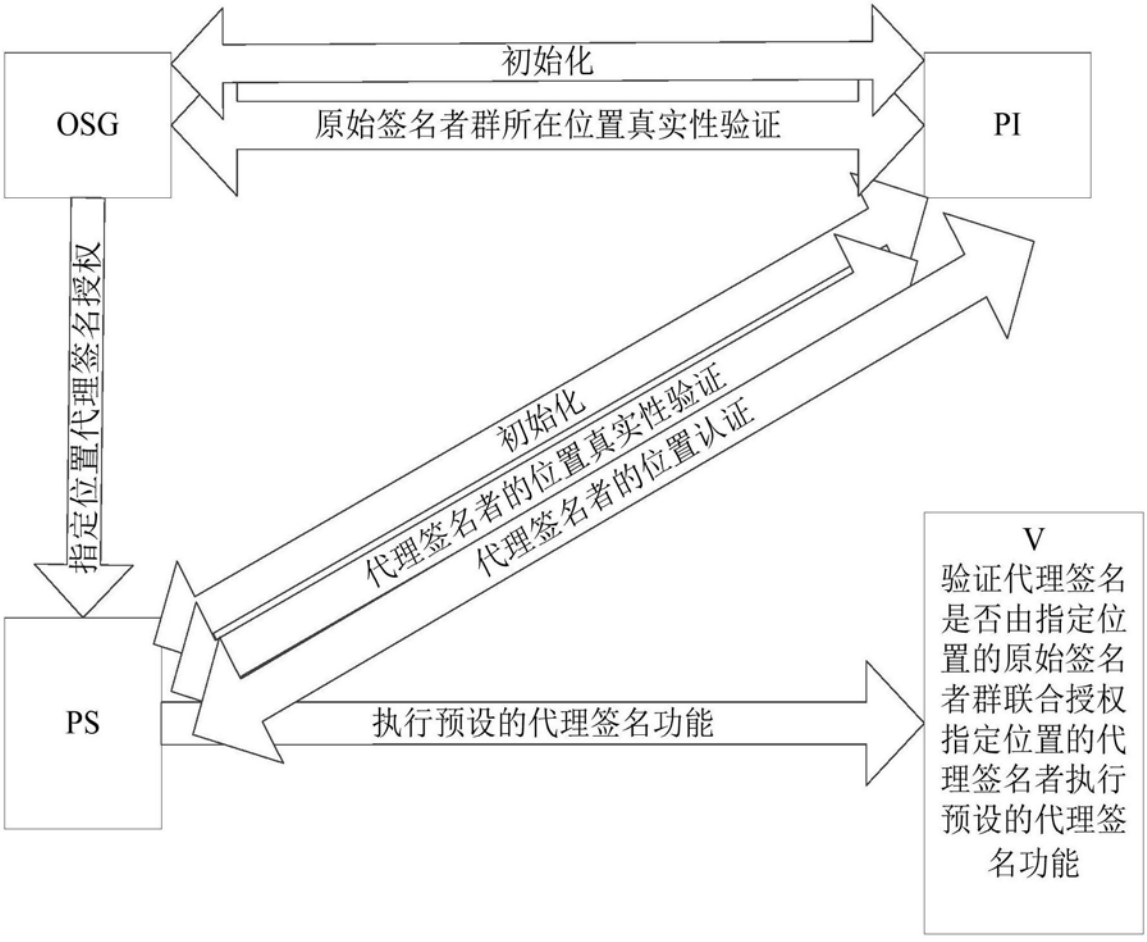

初始化
OSG
原始签名者群所在位置真实性验证
PI
指定位置代理签名授权
初始化
代理签名者的位置真实性验证
代理签名者的位置认证
V
验证代理签名是否由指定位置的原始签名者群联合授权指定位置的代理签名者执行预设的代理签名功能
PS
执行预设的代理签名功能

图2

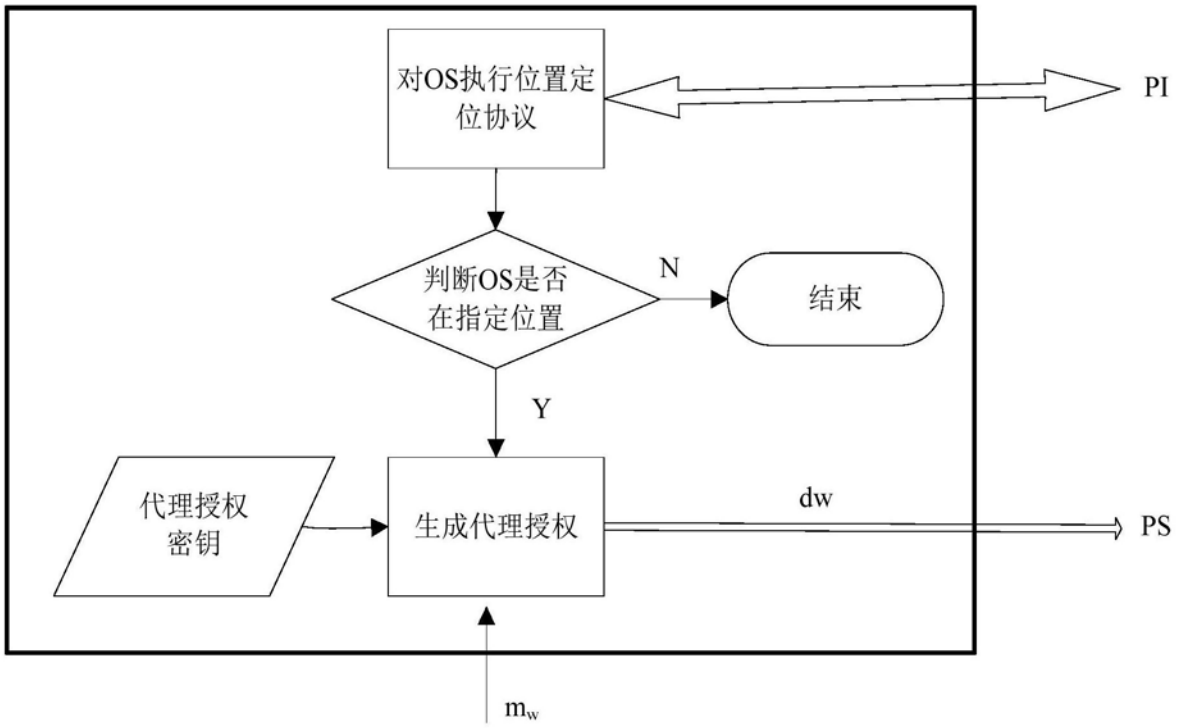

对OS执行位置定位协议
PI
判断OS是否在指定位置
N
结束
Y
代理授权密钥
生成代理授权
dw
PS
m_w

图3

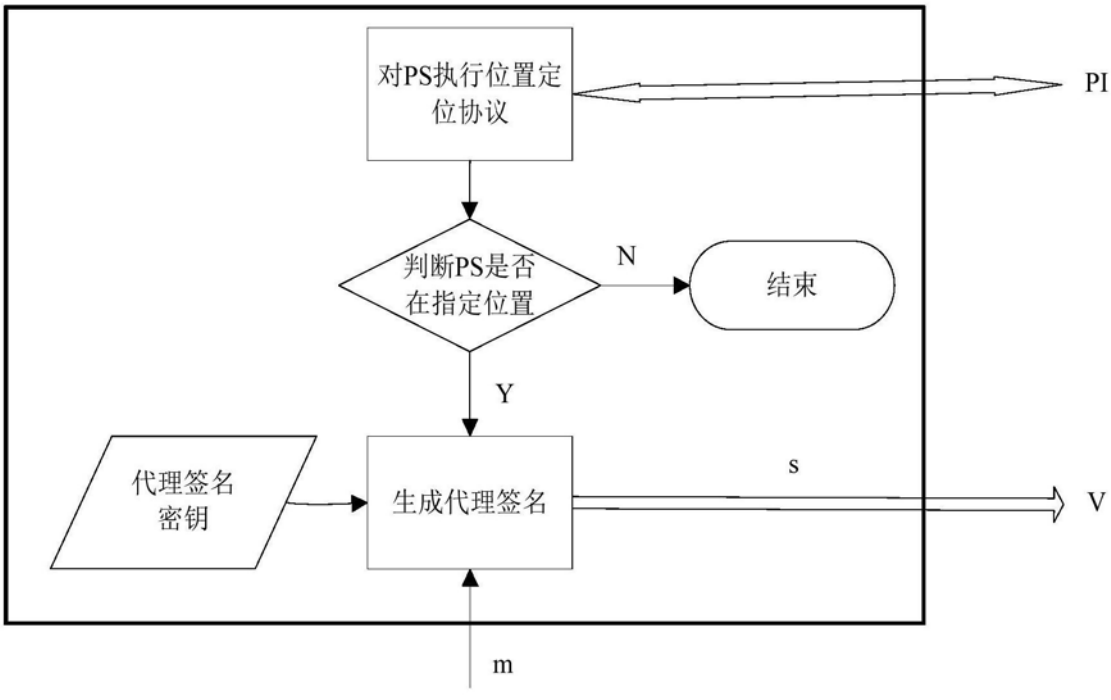

对PS执行位置定位协议
PI
判断PS是否在指定位置
N
结束
Y
代理签名密钥
生成代理签名
s
V
m

图4