(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106031084 A
(43)申请公布日 2016.10.12

(21)申请号 201480075371.4

(22)申请日 2014.11.13

(30)优先权数据
10-2014-0018210 2014.02.18 KR

(85)PCT国际申请进入国家阶段日
2016.08.11

(86)PCT国际申请的申请数据
PCT/KR2014/010930 2014.11.13

(87)PCT国际申请的公布数据
WO2015/126037 KO 2015.08.27

(71)申请人 稀客股份有限公司
地址 韩国首尔市

(72)发明人 洪起隆

(74)专利代理机构 北京康盛知识产权代理有限公司 11331
代理人 张良

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)

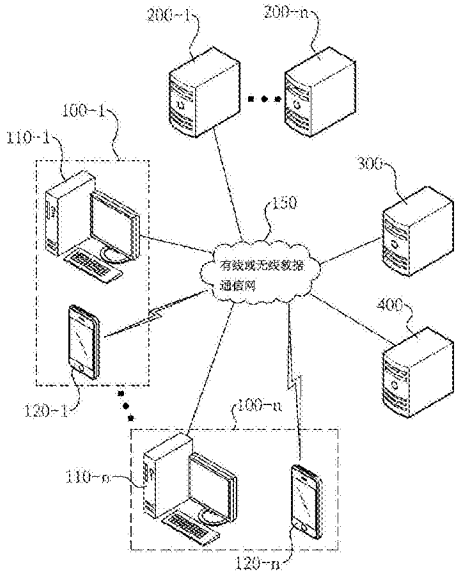
权利要求书5页 说明书13页 附图6页

(54)发明名称

利用一次性随机密钥的本人确认及防盗用系统及方法

(57)摘要

本发明涉及在线执行本人认证的本人认证系统，更详细地，涉及向用户终端部提供当请求本人认证时所发放的认证密钥(C)，借助一次性随机密钥，生成上述认证密钥(C)的认证对应值并执行本人认证，由此，即使上述认证密钥(C)被泄露或被夺获，上述认证密钥(C)也不会被盗用，并安全执行本人认证，从而可防止本人认证及上述认证密钥(C)被盗用的本人确认及防盗用系统及方法。



CN 106031084 A

1.一种利用一次性随机密钥的本人确认及防盗用系统,其特征在于,包括:

用户终端部,当通过任意服务服务器利用需要进行本人认证的服务时,接收本人认证消息,上述本人认证消息包含基于本人认证请求的认证密钥(C),在借助随机生成的作为一次性随机密钥的安全密钥(R)对上述认证密钥(C)进行异或运算来生成认证对应值(eC)之后,传输上述认证对应值(eC);以及

本人认证服务器部,对上述本人认证请求生成固有的认证密钥(C),向上述用户终端部传输包含上述认证密钥(C)的本人认证消息,与其响应地,从上述用户终端部接收认证对应值(eC),借助安全密钥(R)生成与上述认证对应值(eC)相对应的验证密钥(C′),借助所生成的验证密钥(C′)对上述认证对应值(eC)进行验证来执行本人认证。

2.根据权利要求1所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,上述用户终端部包括:

计算机终端,连接上述服务服务器,请求基于利用上述服务的本人认证;以及

便携式终端,接收基于上述本人认证请求的上述本人认证消息,在借助上述安全密钥(R)对认证密钥(C)进行异或运算来生成上述认证对应值(eC)之后,向上述本人认证服务器传输上述认证对应值(eC)。

3.根据权利要求1所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,上述用户终端部包括:

便携式终端,接收基于上述本人认证请求的上述本人认证消息,在借助上述安全密钥(R)对上述认证密钥(C)进行异或运算来生成上述认证对应值(eC)之后,显示上述认证对应值(eC);以及

计算机终端,连接上述服务服务器,请求基于利用上述服务器的本人认证,接收用户所输入的显示在上述便携式终端的上述认证对应值(eC)并向上述本人认证服务器传输上述认证对应值(eC)。

4.根据权利要求2或3所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,上述便携式终端生成上述安全密钥(R)并向安全认证服务器部提供上述安全密钥(R)。

5.根据权利要求2或3所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,上述本人认证服务器部生成上述安全密钥(R)并向便携式认证终端提供上述安全密钥(R)。

6.根据权利要求2或3所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述便携式终端在以上述便携式终端识别信息及电话号码中的1种以上对上述认证密钥(C)进行异或运算之后,借助上述安全密钥(R)进行异或运算来生成上述认证对应值(eC),

上述本人认证服务器在接收上述认证对应值(eC)时生成上述安全密钥(R),并对上述便携式终端识别信息及电话号码中的1种以上执行异或运算来生成验证密钥(C′)。

7.根据权利要求2或3所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述本人认证服务器部借助包含作为一次性随机密钥的随机选择密钥(K)的2个以上的一次性随机密钥生成上述认证密钥(C),

对上述一次性随机密钥中的除上述选择随机密钥之外的其他一次性随机密钥执行异或运算来计算出作为验证密钥(C′)的选择随机密钥(K′),判断上述选择随机密钥(K)与所计算出的选择随机密钥(K′)是否一致,由此验证上述认证对应值(eC)。

8.根据权利要求6所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述本人认证服务器部借助包含作为一次性随机密钥的随机选择密钥(K)的2个以上的一次性随机密钥生成上述认证密钥(C),

对上述一次性随机密钥中的除上述选择随机密钥之外的其他一次性随机密钥执行异或运算来计算出作为验证密钥(C′)的选择随机密钥(K′),判断上述选择随机密钥(K)与所计算出的选择随机密钥(K′)是否一致,由此验证上述认证对应值(eC)。

9.根据权利要求2或3所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述便携式终端通过预先确定的比特选择方式从所生成的上述认证对应值中仅提取任意的比特数并向本人认证服务器部传输上述比特数,

上述本人认证服务器部在传输包含上述认证密钥(C)的本人认证消息之后生成上述认证密钥(C)和上述安全密钥(R),在对上述便携式终端识别信息及电话号码中的1种以上进行异或运算来计算出认证对应值(eC)之后,通过上述比特选择方式从上述认证对应值(eC)中仅提取上述比特数来生成上述验证密钥(C′)。

10.根据权利要求6所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述便携式终端通过预先确定的比特选择方式从所生成的上述认证对应值中仅提取任意的比特数并向本人认证服务器部传输上述比特数,

上述本人认证服务器部在传输包含上述认证密钥(C)的本人认证消息之后生成上述认证密钥(C)和上述安全密钥(R),在对上述便携式终端识别信息及电话号码中的1种以上进行异或运算来计算出认证对应值(eC)之后,通过上述比特选择方式从上述认证对应值(eC)中仅提取上述比特数来生成上述验证密钥(C′)。

11.根据权利要求2或3所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述本人认证消息为短消息服务、长消息服务及多媒体消息服务消息中的1种,

上述本人认证服务器部向上述便携式终端传输上述本人认证消息。

12.根据权利要求2或3所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述本人认证消息为短消息服务、长消息服务及多媒体消息服务消息中的1种,

上述本人认证服务器部向服务服务器或以往认证系统提供上述认证密钥(C),使得上述服务服务器或以往认证系统向上述便携式终端传输上述本人认证消息。

13.根据权利要求10所述的利用一次性随机密钥的本人确认及防盗用系统,其特征在于,

上述便携式终端显示上述认证对应值(eC),

上述计算机终端接收用户的上述认证对应值(eC)并向上述本人认证服务器部传输上述认证对应值(eC)。

14.根据权利要求13所述的利用一次性随机密钥的本人确认及防盗用系统，其特征在于，上述计算机终端通过服务服务器部向上述本人认证服务器部传输上述认证对应值(eC)。

15.根据权利要求1所述的利用一次性随机密钥的本人确认及防盗用系统，其特征在于，

上述用户终端部包括计算机终端以及便携式终端，

上述本人认证消息为包含认证密钥(C)的二维码，上述本人认证服务器部向上述计算机终端传输上述本人认证消息，

上述计算机终端显示上述本人认证消息，

上述便携式终端通过对作为显示在上述计算机终端的本人认证消息的二维码进行扫描来取得上述认证密钥(C)，借助所取得的认证密钥(C)和安全密钥(R)生成上述认证对应值(eC)。

16.一种利用一次性随机密钥的本人确认及防盗用方法，其特征在于，包括：

本人认证消息发送步骤，当以往认证系统通知本人认证信息成功一致时，本人认证服务器部生成对本人认证请求的固有的认证密钥(C)，向用户终端部传输包含所生成的认证密钥(C)的本人认证消息；

传输认证对应值步骤，上述用户终端部接收上述本人认证消息，在借助安全密钥(R)对上述认证密钥(C)进行异或运算来生成认证对应值(eC)之后，向上述本人认证服务器部传输上述认证对应值(eC)；以及

本人认证步骤，上述本人认证服务器部借助上述安全密钥(R)对上述认证对应值(eC)进行异或运算来生成验证密钥(C′)，借助所生成的验证密钥(C′)验证上述认证对应值(eC)。

17.根据权利要求16所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，上述本人认证消息发送步骤包括：

认证密钥生成步骤，响应于上述本人认证请求，借助包含作为一次性随机密钥的随机选择密钥(K)的2个以上的一次性随机密钥生成上述认证密钥(C)；

本人认证消息生成步骤，生成包含所生成的上述认证密钥(C)的本人认证消息；以及

本人认证消息传输步骤，向上述用户终端部传输上述本人认证消息。

18.根据权利要求16所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，

上述本人认证消息发送步骤包括：

认证密钥生成步骤，响应于上述本人认证请求，借助包含作为一次性随机密钥的随机选择密钥(K)的2个以上的一次性随机密钥生成上述认证密钥(C)；

本人认证消息生成步骤，生成包含所生成的上述认证密钥(C)的本人认证消息；以及

本人认证消息传输步骤，向上述用户终端部传输本人认证消息，

上述本人认证步骤包括：

验证密钥生成步骤，对上述一次性随机密钥中的除上述选择随机密钥之外的其他一次性随机密钥执行异或运算来计算出作为验证密钥(C′)的选择随机密钥(K′)；以及

认证步骤，判断上述选择随机密钥(K)与所计算出的选择随机密钥(K′)是否一致，由此

验证上述认证对应值(eC)。

19.根据权利要求16所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，上述传输认证对应值步骤包括：

认证密钥取得步骤，从本人认证消息取得认证密钥(C)；

安全密钥取得步骤，取得上述安全密钥(R)；以及

认证对应值生成步骤，借助上述认证密钥(C)和安全密钥(R)生成认证对应值。

20.根据权利要求19所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，在上述认证对应值生成步骤中，用户终端部的便携式终端对自身的固有识别信息及电话号码中的1种以上执行异或运算来生成上述认证对应值(eC)。

21.根据权利要求16、19或20所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，

在上述认证对应值生成步骤中，用户终端部的便携式终端通过预先确定的比特选择方式，在所生成的上述认证对应值(eC)中提取任意比特数的任意比特来以最终认证对应值(eC)进行传输，

上述本人认证服务器部在上述本人认证过程中对于上述验证密钥(C′)判断仅提取通过上述比特选择方式选择的比特的最终验证密钥(C′)和上述最终认证对应值(eC)是否相同，由此执行本人认证。

22.根据权利要求21所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，随机确定所提取的上述比特数及比特。

23.根据权利要求19所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，

在上述本人认证消息发送过程中，本人认证服务器部以移动通信消息向用户终端部的便携式终端传输上述本人认证消息，

在上述传输认证对应值过程中，上述便携式终端生成上述认证对应值(eC)并向上述本人认证服务器部传输上述认证对应值(eC)。

24.根据权利要求19所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，

在上述本人认证消息发送过程中，本人认证服务器部以移动通信消息向用户终端部的便携式终端传输上述本人认证消息，

上述传输认证对应值过程包括：

显示步骤，上述便携式终端借助上述本人认证消息的认证密钥(C)及上述安全密钥(R)生成上述认证对应值(eC)并显示认证对应值(eC)；以及

传输认证对应值步骤，上述用户终端的计算机终端接收用户输入的显示在上述便携式终端的认证对应值并向本人认证服务器部传输上述认证对应值。

25.根据权利要求19所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，

在上述本人认证消息发送过程中，上述本人认证服务器部以二维码形态向用户终端部的计算机终端传输上述本人认证消息，

上述传输认证对应值过程包括：

显示步骤，上述计算机终端以上述二维码的形态显示本人认证消息；以及

传输认证对应值步骤，上述便携式终端对显示在上述计算机终端的二维码进行扫描来生成本人认证对应值(eC)，向上述本人认证服务器部传输所生成的认证对应值(eC)。

26.根据权利要求16至20、22至25中任一项所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，在上述传输认证对应值过程中，便携式终端在生成上述安全密钥(R)之后向上述本人认证服务器部提供上述安全密钥(R)。

27.根据权利要求16至20、22至25中任一项所述的利用一次性随机密钥的本人确认及防盗用方法，其特征在于，在本人认证服务器部生成上述认证密钥(C)之后生成上述安全密钥(R)并向便携式终端提供上述安全密钥(R)。

利用一次性随机密钥的本人确认及防盗用系统及方法

技术领域

[0001] 本发明涉及在线执行本人认证的本人认证系统，更详细地，涉及向用户终端部提供当请求本人认证时所发放的认证密钥C，借助一次性随机密钥，生成上述认证密钥C的认证对应值并执行本人认证，由此，即使上述认证密钥C被泄露或被夺获，上述认证密钥C也不会被盗用，并安全执行本人认证，从而可防止本人认证及上述认证密钥C被盗用的本人确认及防盗用系统及方法。

背景技术

[0002] 目前的互联网技术发展到了已构成无论在何时何地均可连接互联网的云计算环境。随着构建上述云计算环境，普遍发生在线使用信用信息的情况。上述信用信息广泛用于在线加入会员、在线购买商品及通过金融机关的经济生活领域等。

[0003] 由此，黑客盗取在线使用的信用信息，并盗用所盗取的信用信息，从而损害个人产生经济。

[0004] 因此，互联网系统为了防止黑客盗取个人的信用信息而适用多种认证系统。上述认证系统主要适用确认利用网络上的任意服务器的用户是否为自己的本人认证(或者，被称为“用户认证，“本人确认”等)系统。

[0005] 通常，本人认证系统当任意用户请求如会员登录及变更、结算及转账等的任意服务时，用户为了确认对于对应服务的适当的用户，即，为了确认是否为本人，向预先登录从用户输入的用户输入信息和对于上述用户的用户信息的如移动通信系统、信用评价系统及公认认证系统等的以往的认证系统(以下，称之为“以往认证系统”)传输用户输入信息，并比较上述用户信息和上述用户输入信息来执行本人信息认证，向已认证本人信息的用户的移动通信终端传输包含认证号码的本人认证消息，通过用户的计算机，在规定时间内从用户接收上述认证号码，并判断上述认证号码与发放的认证号码是否一致，由此执行本人认证。通常，根据本人认证方式，上述用户输入信息可以为用户的身份证号，也可以为用户所有的卡号、CVC及有效期间等。

[0006] 如上所述，以往本人认证系统得输入如身份证号、卡号等的用户的重要个人信息及信用信息，从而存在因存储器被盗取等原因而导致用户的身份证号等的信用信息泄露的问题。

[0007] 并且，以往本人认证系统存在可被导出包含用于本人认证的认证号码的认证信息的第三者盗用的问题。

[0008] 为了防止上述问题，在韩国公开专利公报第10-2013-0084727号(以下，称之为“现有专利1”)及韩国公开专利公报第10-2014-0003353号(以下，称之为“以往专利2”)中公开了预先选择在用户接收的认证消息的认证号码的位数中需要使用的位数，且仅输入与用户预先选择的位数相对应的号码，从而提高安全性的方式。

[0009] 并且，为了解决上述以往本人认证系统的问题，在韩国授权专利第10-1321828号(以下，称之为“现有专利3”)中公开了在传输本人认证消息之前，发送包含任意网页URL的

本人确认消息，并使用户连接上述本人确认消息的URL之后，从用户接收密码，仅在上述接收的密码和以往登录的密码相同的情况下，传输本人认证消息的方式。

[0010] 但是，上述现有专利仅在认证号码的输入方式存在一部分差异，且依然适用简单移动通信消息方式，从而存在对短消息服务/长消息服务/多媒体消息服务等的移动通信消息夺获及存储器盗取等方面脆弱的问题。

[0011] 因此，现有专利也存在可被盗取并被第三者盗用的问题。

[0012] 而且，上述现有专利3存在如下问题，即，传输包含URL的文字消息，由此存在用户会识别成钓鱼消息的忧虑，在用户将上述文字消息认为是钓鱼消息而删除的情况下，用户会感到不便或无法接收服务。

发明内容

[0013] 技术问题

[0014] 因此，本发明的目的在于，提供向用户终端部提供当请求本人认证时所发放的认证密钥C，借助一次性随机密钥，生成上述认证密钥C的认证对应值并执行本人认证，由此，即使上述认证密钥C被泄露或被夺获，上述认证密钥C也不会被盗用，并安全执行本人认证，从而可防止本人认证及上述认证密钥C的盗用的本人确认及防盗用系统及方法。

[0015] 解决问题的方案

[0016] 用于实现上述目的的本发明的利用一次性随机密钥的本人确认及防盗用系统的特征在于，包括：用户终端部，当通过任意服务服务器利用需要进行本人认证的服务时，接收本人认证消息，上述本人认证消息包含基于本人认证请求的认证密钥C，在借助随机生成的作为一次性随机密钥的安全密钥R对上述认证密钥C进行异或运算来生成认证对应值eC之后，传输上述认证对应值eC；以及本人认证服务器部，对上述本人认证请求生成固有的认证密钥C，向上述用户终端部传输包含上述认证密钥C的本人认证消息，与其响应地，从上述用户终端部接收认证对应值eC，借助生成安全密钥R与上述认证对应值eC相对应的验证密钥C′，借助所生成的验证密钥C′对上述认证对应值eC进行验证来执行本人认证。

[0017] 本发明的特征在于，上述用户终端部包括：计算机终端，连接上述服务服务器，请求基于利用上述服务的本人认证；以及便携式终端，接收基于上述本人认证请求的上述本人认证消息，在借助上述安全密钥R对认证密钥C进行异或运算来生成上述认证对应值eC之后，向上述本人认证服务器传输上述认证对应值eC。

[0018] 本发明的特征在于，上述用户终端部包括：便携式终端，接收基于上述本人认证请求的上述本人认证消息，在借助上述安全密钥R对上述认证密钥C进行异或运算来生成上述认证对应值eC之后，显示上述认证对应值eC；以及计算机终端，连接上述服务服务器，请求基于利用上述服务器的本人认证，接收用户所输入的显示在上述便携式终端的上述认证对应值eC并向上述本人认证服务器传输上述认证对应值eC。

[0019] 本发明的特征在于，上述便携式终端生成上述安全密钥R并向安全认证服务器部提供上述安全密钥R。

[0020] 本发明的特征在于，上述安全认证服务器部生成上述安全密钥R并向便携式认证终端提供上述安全密钥R。

[0021] 本发明的特征在于，上述便携式终端在以上述便携式终端识别信息及电话号码中

的1种以上对上述认证密钥C进行异或运算之后，借助上述安全密钥R进行异或运算来生成上述认证对应值eC，上述本人认证服务器在接收上述认证对应值eC时生成上述安全密钥R，并对上述便携式终端识别信息及电话号码中的1种以上执行异或运算来生成验证密钥C′。

[0022] 本发明的特征在于，上述本人认证服务器部借助包含作为一次性随机密钥的随机选择密钥K的2个以上的一次性随机密钥生成上述认证密钥C，对上述一次性随机密钥中的除作为任意选择的一个一次性随机密钥的选择随机密钥之外的其他一次性随机密钥执行异或运算来生成与上述选择随机密钥相对应的验证密钥C′。

[0023] 本发明的特征在于，上述本人认证服务器部借助包含作为一次性随机密钥的随机选择密钥K的2个以上的一次性随机密钥生成上述认证密钥C，对上述一次性随机密钥中的除作为任意选择的一个一次性随机密钥的选择随机密钥之外的其他一次性随机密钥执行异或运算来生成与上述选择随机密钥相对应的验证密钥C′。

[0024] 本发明的特征在于，上述便携式终端从所生成的上述认证对应值中仅提取任意的比特数并向本人认证服务器部传输上述比特数，上述本人认证服务器部在传输包含上述认证密钥C的本人认证消息之后生成上述认证密钥C和上述安全密钥R进行异或运算来计算出认证对应值eC之后，从上述认证对应值eC中仅提取上述比特数来生成上述验证密钥C′。

[0025] 本发明的特征在于，上述便携式终端从所生成的上述认证对应值中仅提取任意的比特数并向本人认证服务器部传输上述比特数，上述本人认证服务器部在传输包含上述认证密钥C的本人认证消息之后生成上述认证密钥C和上述安全密钥R，在对上述便携式终端识别信息及电话号码中的1种以上进行异或运算来计算出认证对应值eC之后，从上述认证对应值eC中仅提取上述比特数来生成上述验证密钥C′。

[0026] 本发明的特征在于，上述本人认证消息为短消息服务(SMS，Short Message Service)、长消息服务(LMS，Long Message Service)及多媒体消息服务(MMS，Multimedia Message Service)消息中的1种，上述本人认证服务器部向上述便携式终端传输上述本人认证消息。

[0027] 本发明的特征在于，上述本人认证消息为短消息服务、长消息服务及多媒体消息服务消息中的1种，上述本人认证服务器部向服务服务器或以往认证系统提供上述认证密钥C，使得上述服务服务器或以往认证系统向上述便携式终端传输上述本人认证消息。

[0028] 本发明的特征在于，上述便携式终端显示上述认证对应值eC，上述计算机终端接收用户的上述认证对应值eC并向上述本人认证服务器部传输上述认证对应值eC。

[0029] 本发明的特征在于，上述计算机终端通过服务服务器部向上述本人认证服务器部传输上述认证对应值eC。

[0030] 本发明的特征在于，上述用户终端部包括计算机终端以及便携式终端，上述本人认证消息为包含认证密钥C的二维码，上述本人认证服务器部向上述计算机终端传输上述本人认证消息，上述计算机终端显示上述本人认证消息，上述便携式终端通过对作为显示在上述计算机终端的本人认证消息的二维码进行扫描来取得上述认证密钥C，借助所取得的认证密钥C和生成安全密钥R上述认证对应值eC。

[0031] 用于实现上述目的的本发明的利用一次性随机密钥的本人确认及防盗用方法的特征在于，包括：本人认证消息发送步骤，当以往认证系统通知本人认证信息成功一致时，本人认证服务器部生成对本人认证请求的固有的认证密钥C，向用户终端部传输包含所生

成的认证密钥C的本人认证消息;传输认证对应值步骤,上述用户终端部接收上述本人认证消息,在借助安全密钥R对上述认证密钥C进行异或运算来生成认证对应值eC之后,向上述本人认证服务器部传输上述认证对应值eC;以及本人认证步骤,上述本人认证服务器部借助上述安全密钥R对上述认证对应值eC进行异或运算来生成验证密钥C′,借助所生成的验证密钥C′验证上述认证对应值eC。

[0032] 本发明的特征在于,上述本人认证消息发送步骤包括:认证密钥生成步骤,响应于上述本人认证请求,借助一次性随机密钥生成上述认证密钥C;本人认证消息生成步骤,生成包含所生成的上述认证密钥C的本人认证消息;以及本人认证消息传输步骤,向上述用户终端部传输上述本人认证消息。

[0033] 本发明的特征在于,上述本人认证消息发送步骤包括:认证密钥生成步骤,响应于上述本人认证请求,借助包含作为一次性随机密钥的随机选择密钥K的2个以上的一次性随机密钥生成上述认证密钥C;本人认证消息生成步骤,生成包含所生成的上述认证密钥C的本人认证消息;以及本人认证消息传输步骤,向上述用户终端部传输本人认证消息,上述本人认证步骤包括:验证密钥生成步骤,对上述一次性随机密钥中的除作为任意选择的一个一次性随机密钥的选择随机密钥之外的其他一次性随机密钥执行异或运算来计算出作为验证密钥C′的选择随机密钥K′;以及认证步骤,判断上述验证密钥C′与所生成的认证密钥C是否一致来执行验证。

[0034] 本发明的特征在于,上述传输认证对应值步骤包括:认证密钥取得步骤,从本人认证消息取得认证密钥C;安全密钥取得步骤,取得上述安全密钥R;以及认证对应值生成步骤,借助上述认证密钥C和生成安全密钥R认证对应值。

[0035] 本发明的特征在于,在上述认证对应值生成步骤中,用户终端部的便携式终端对自身的固有识别信息及电话号码中的1种以上执行异或运算来生成上述认证对应值eC。

[0036] 本发明的特征在于,在上述认证对应值生成步骤中,用户终端部的便携式终端通过预先确定的比特选择方式,在所生成的上述认证对应值eC中提取任意比特数的任意比特来以最终认证对应值eC进行传输,上述本人认证服务器部在上述本人认证过程中判断仅提取通过上述比特选择方式选择的比特的验证密钥C′和上述认证对应值eC是否相同,由此执行本人认证。

[0037] 本发明的特征在于,随机确定所提取的上述比特数及比特。

[0038] 本发明的特征在于,在上述本人认证消息发送过程中,本人认证服务器部以移动通信消息向用户终端部的便携式终端传输上述本人认证消息,在上述传输认证对应值过程中,上述便携式终端生成上述认证对应值eC并向上述本人认证服务器部传输上述认证对应值eC。

[0039] 本发明的特征在于,在上述本人认证消息发送过程中,本人认证服务器部以移动通信消息向用户终端部的便携式终端传输上述本人认证消息,上述传输认证对应值过程包括:显示步骤,上述便携式终端借助上述本人认证消息的认证密钥C及上述生成安全密钥R上述认证对应值eC并显示认证对应值eC;以及传输认证对应值步骤,上述用户终端的计算机终端接收用户输入的显示在上述便携式终端的认证对应值并向本人认证服务器部传输上述认证对应值。

[0040] 本发明的特征在于,在上述本人认证消息发送过程中,上述本人认证服务器部以

二维码形态向用户终端部的计算机终端传输上述本人认证消息，上述传输认证对应值过程包括：显示步骤，上述计算机终端以上述二维码的形态显示本人认证消息；以及传输认证对应值步骤，上述便携式终端对显示在上述计算机终端的二维码进行扫描来生成本人认证对应值eC，向上述本人认证服务器部传输所生成的认证对应值eC。

[0041] 本发明的特征在于，在上述传输认证对应值过程中，便携式终端在生成上述安全密钥R之后向上述本人认证服务器部提供上述安全密钥R。

[0042] 本发明的特征在于，在本人认证服务器部生成上述认证密钥C之后生成上述安全密钥R并向便携式终端提供上述安全密钥R。

[0043] 发明的效果

[0044] 本发明具有如下效果，即本发明可适用于以往本人认证系统，但是不使用身份证号等的非常敏感的用户个人信息及信用信息，在不输入任何信息的情况下，可通过随机生成的一次性安全密钥执行本人认证，因此，可防止用户的个人信息及信用信息被泄露或者可防止第三者的盗用。

[0045] 并且，本发明具有如下效果，即，本人认证服务器向用户终端部提供认证密钥C，向本人认证服务器传输通过随机生成的一次性安全密钥R对上述认证密钥C进行异或运算的认证对应值来执行本人认证，因此，即使包含认证密钥C的认证消息被泄露或被夺获，第三者也无法盗用认证密钥C及手机号码等。

附图说明

[0046] 图1为示出本发明的利用一次性随机密钥的本人确认及防盗用系统的结构的图。

[0047] 图2为示出本发明利用一次性随机密钥的本人确认及防盗用系统的便携式终端的结构的图。

[0048] 图3为示出本发明的利用一次性随机密钥的本人确认及防盗用系统的本人认证服务器的结构的图。

[0049] 图4为示出本发明第一实施例的利用移动通信消息及一次性随机密钥的本人确认及防盗用方法的流程图。

[0050] 图5为示出本发明第二实施例的利用移动通信消息及一次性随机密钥的本人确认及防盗用方法的流程图。

[0051] 图6为示出本发明第三实施例的利用二维码及利用一次性随机密钥的本人确认及防盗用方法的流程图。

[0052] 图7为示出本发明第四实施例的利用二维码及一次性随机密钥的本人确认及防盗用方法的流程图。

具体实施方式

[0053] 以下，参照附图，说明本发明的利用一次性随机密钥的本人确认及防盗用系统的结构及运行，并说明在上述系统中的本人确认及防盗用方法。

[0054] 图1为示出本发明的利用一次性随机密钥的本人确认及防盗用系统的结构的图。

[0055] 参照图1，本发明的本人确认及防盗用系统包括用户终端部100、服务器200、本人认证服务部300及以往认证系统400。

[0056] 上述用户终端部100、服务器200、本人认证服务器300及以往认证系统400通过有线或无线数据通信网150相连接，由此执行数据通信。

[0057] 上述有线或无线通信网150为包括可进行2G(2Generation)、3G(3Generation)、4G(4Generation:4G＝LTE(Long Term Evolution))等的数据通信的移动通信网、无线保真(WiFi)网、广域网(WAN,Wide Area Network)及局域网(LAN,Local Area Network)等相结合的互联网中的1个以上的通信网。

[0058] 用户终端部100包括计算机终端110及便携式终端120。

[0059] 计算机终端110可以为个人计算机(PC,Personal Computer)、笔记本等，也可以为智能手机、智能触控板等的智能设备。在上述计算机终端110为智能手机及智能触控板等的智能设备的情况下，计算机终端110可以为便携式终端120。即，在用户所持有的终端为智能设备的情况下，1个终端可以为计算机终端，也可以为便携式终端。

[0060] 计算机终端110通过有线或无线通信网150与任意服务器200相连接，由此可接收从上述相连接的服务器200所提供的多种服务，在接受上述服务的过程中，在执行需要本人认证的服务的情况下，接收用户的同意之后进行本人认证。

[0061] 计算机终端110可根据本发明的实施例，接收包含从本人认证服务器部300接收的认证密钥C的本人认证消息并显示，且可从用户接收认证对应值eC并通过服务器200向本人认证服务器部300提供，也可直接向本人认证服务器部300传输上述认证对应值eC。

[0062] 便携式终端120为具有自身固有的识别信息(以下，称之为“便携式终端识别信息”)的终端，根据实施例，便携式终端120可以为与2G、3G及4G移动通信网中的1个以上相连接的手机、智能手机、智能触控板等的通信终端。

[0063] 根据第一实施例及第三实施例，便携式终端120从本人认证服务器部300接收包含认证密钥C的本人认证消息，并检测所接受的本人认证消息的认证密钥C，随机生成的一次性密钥R(以下，称之为“安全密钥R”)之后，对检测的认证密钥C和所生成的安全密钥R适用下述数学式1来生成认证对应值eC。

[0064] 数学式1

[0065] $$eC = C \oplus R$$

[0066] 其中，C为认证密钥，R为安全密钥。

[0067] 并且，根据第二实施例，便携式终端120从本人认证服务器部300接收包含认证密钥C的本人认证消息，并检测所接受的本人认证消息的认证密钥C，从本人认证服务器部300接收随机生成的安全密钥R之后，借助上述数学式1，对上述检测的认证密钥和所接受的随机密钥R生成认证对应值eC。

[0068] 并且，根据第三实施例，便携式终端120接收显示在计算机终端110的本人认证消息的认证密钥C，在生成作为随机(Random)生成的一次性随机密钥的安全密钥R之后，对检测的认证密钥C和所生成的安全密钥R适用上述数学式1来生成认证对应值eC。

[0069] 并且，根据第四实施例，便携式终端120接收在计算机终端110显示的本人认证消息的认证密钥C，在接受从本人认证服务器部300随机生成的安全密钥R之后，借助上述数学式1对上述检测的认证密钥和接收的随机密钥R生成认证对应值eC。

[0070] 根据实施例，便携式终端120可直接向本人认证服务器部300传输所生成的认证对应值eC，也可由用户通过在计算机终端110中输入的服务器200或直接向本人认证服务器部

300传输。

[0071] 并且，如上述第一实施例和第三实施例，上述便携式终端120可向本人认证服务器部300提供在生成安全密钥R的情况下所生成的安全密钥R。

[0072] 并且，如下述数学式2，便携式终端120可选择性适用便携式终端120的便携式终端识别信息及电话号码中的1种以上来生成认证对应值eC。

[0073] 数学式2

[0074] $$eC = C(\oplus MID)(\oplus TNO)\oplus R$$

[0075] 其中，MID为Mobile Identification的缩略语，MID为如电子序列号(ESN，Electronic Serial Number)及国际移动设备标识(IMEI，International Mobile Equipment Identify)等的便携式终端识别信息，TNO为便携式终端120的电话号码。而且，()为可选择性使用的信息。

[0076] 并且，便携式终端120借助在如下述数学式3生成的认证对应值eC中，预先设定的比特选择方式S[]提取任意比特数的比特，并可将上述比特作为最终认证对应值来传输。

[0077] 数学式3

[0078] $$eC = S[C(\oplus MID)(\oplus TNO)\oplus R, n]$$

[0079] 其中，n为所要选择的比特数，S为Select的缩略语并根据预先确定n比特数的选择方式选择，由此生成认证对应值eC。

[0080] 当选择上述n比特时，便携式终端120和本人认证服务器部300可借助预先知道的一次性随机密钥提取随机位数的比特。

[0081] 服务器200向通过有线或无线数据通信网150相连接的用户终端部100的计算机终端110提供包含需要进行本人认证的服务的多种服务，当执行需要本人认证的服务时，向计算机终端110提供本人认证请求机构，当从计算机终端110发生本人认证请求时，向本人认证服务器部300请求本人认证，若成功进行基于本人认证请求的本人认证，则向计算机终端110提供对应服务。

[0082] 以往认证系统400为执行以往的本人认证的认证系统，以往认证系统400可以为移动通信系统、信用评价系统及公认认证系统等。上述通过以往认证系统400的认证请求过程为公知技术，因此将省略对其的详细说明。

[0083] 当从服务器200发生本人认证请求时，本人认证服务器部300向以往认证系统400传输由用户输入的用户输入信息，当接收对基于上述本人认证请求的上述用户输入信息的提供的通知本人信息相同接收时，生成认证密钥C，并向用户终端部100传输包含所生成的认证密钥C的本人认证消息，根据本发明的第二实施例及第四实施例，向用户终端部100的便携式终端120提供安全密钥R。

[0084] 上述认证密钥C可以为根据本发明的实施例随机生成的1个一次性随机密钥K，如下述数学式4所示，也可借助随机生成的2个以上的一次性随机密钥K、R1生成。

[0085] 数学式4

[0086] $$C = K \oplus R1$$

[0087] 其中，K及R1为一次性随机密钥。

[0088] 并且，根据本发明的第二实施例及第四实施例，本人认证服务器部300对所发生的

本人认证请求生成安全密钥R，并向对应用户终端部100的便携式终端120提供上述安全密钥R。

[0089] 在提供认证密钥C之后，本人认证服务器部300监视是否从用户终端部100接收认证对应值eC，当接收认证对应值eC时，生成与认证对应值eC及根据本发明的实施例取得的安全密钥R相对应的验证密钥C′，借助上述验证密钥C′生成上述认证对应值eC，当成功验证时，向服务器200通知本人认证成功，由此向用户终端部100的计算机终端110提供对应服务。相反地，当验证失败时，本人认证服务器部300向服务器200通知本人认证失败，由此服务器200将不提供对应服务。

[0090] 在认证对应值eC借助上述数学式1生成的情况下，本人认证服务器部300借助数学式5生成验证密钥C′，在认证对应值eC借助上述数学式2生成的情况下，本人认证服务器部300借助下述数学式6生成验证密钥C′，在借助上述数学式3生成认证对应值eC的情况下，本人认证服务器部300借助下述数学式7生成验证密钥C′，在借助上述数学式4生成认证密钥C的情况下，本人认证服务器部300借助下述数学式8生成验证密钥C′。

[0091] 数学式5

[0092] $$C' = eC \oplus R$$

[0093] 数学式6

[0094] $$C' = eC(\oplus MID)(\oplus TNO) \oplus R$$

[0095] 数学式7

[0096] $$C' = eC' = S[C(\oplus MID)(\oplus TNO) \oplus R, n]$$

[0097] 数学式8

[0098] $$C' = K' = eC(\oplus MID)(\oplus TNO) \oplus R \oplus R1$$

[0099] 图2为示出本发明的利用一次性随机密钥的本人确认及防盗用系统的便携式终端的结构的图。

[0100] 参照图2，本发明的便携式终端120包括便携式终端控制部10、存储部20、输入部30、显示部40、通信部50及扫描部60。

[0101] 存储部20包括：程序区域，存储用于控制本发明的便携式终端120的运行的控制程序；临时区域，用于存储在上述控制程序执行中所发生的数据；以及数据区域，用于存储用户数据。

[0102] 显示部40用于显示本发明的本人认证消息。

[0103] 输入部30可包括键盘输入装置及触控板等中的1个以上，上述键盘输入装置包括多个文字键及功能键，上述触控板与上述显示部40形成为一体，可借助显示在上述显示部40的用户界面机构选择文字及功能。

[0104] 通信部50通过与有线或无线数据通信网150相连接来与有线或无线数据通信网150相连接的其他装置执行数据通信，上述通信部50包括：移动通信部(未图示)，用于执行利用移动通信网的数据通信；以及无线通信部(未图示)，用于执行利用互联网的数据通信。

[0105] 扫描部60包括摄像头及红外线发送部/接收部等，由此，扫描部60对显示在计算机终端110等的二维码进行扫描并向便携式终端控制部10输出扫描结果。

[0106] 根据实施例，便携式终端控制部10包括：消息处理部11，接收通过通信部50接收的

本人认证消息；认证密钥取得部12，取得从上述消息处理部11及扫描部60扫描的二维码或者通过输入部30取得本人认证消息的认证密钥C；以及认证对应值生成部13，借助上述取得的认证密钥C和根据实施例直接生成或从本人认证服务器部300接收的生成安全密钥R认证对应值eC，由此，便携式终端控制部10控制本发明的整体运行。

[0107] 根据实施例，上述认证对应生成部13可根据数学式1至数学式3生成认证对应值eC。

[0108] 图3为示出本发明的利用一次性随机密钥的本人确认及防盗用系统的本人认证服务器部的结构的图。

[0109] 参照图3，本人认证服务器300包括认证控制部310、存储部340及通信部350。

[0110] 存储部340包括：用户信息数据库，用于存储用户终端部100的用户的信息(以下，称之为“用户信息”)；认证明细数据库，用于存储根据本发明处理的认证处理明细。上述用户信息可包含：1个以上的种子密钥，用于根据本发明的实施例(第二实施例、第四实施例)，对上述用户生成安全密钥R；安全密钥R，根据本发明的实施例(第一实施例、第三实施例)取得；以及用户便携式终端120的便携式终端识别信息及电话号码等。

[0111] 通信部350以有线或无线的方式与有线或无线数据通信网150相连接，由此与有线或无线数据通信网150相连接的其他装置执行数据通信。

[0112] 认证控制部310包括用户登录部320及认证处理部330，认证控制部310用于控制本发明的本人认证服务器部300的整体运行。

[0113] 具体地，用户登录部320向用户终端部100提供会员登录机构，通过上述会员登录机构接收对应用户的用户信息并将上述用户信息存储于存储部340的用户信息数据库，由此以会员登录。

[0114] 认证处理部330对上述以会员登录的用户执行本发明的本人认证及用于防止盗用的本人认证消息生成及对于在上述本人认证消息的认证密钥C的验证。

[0115] 上述认证处理部330包括本人认证消息生成部331、验证密钥生成部332及验证部335。

[0116] 若发生本人认证请求并发生从以往认证系统提供通知本人信息相同，则本人认证消息生成部331生成认证密钥C，在生成包含上述认证密钥C的本人认证消息之后，通过通信部350向对应用户终端部100传输上述本人认证消息。根据实施例，上述本人认证消息能够以通过应用的推送消息及应用消息的方式传输，也能够以短消息服务/长消息服务/多媒体消息服务的方式传输，还能够以互联网消息的方式传输。在以上述应用消息及移动通信消息的方式传输上述本人认证消息的情况下，可向便携式终端120传输本人认证消息，在以互联网消息传输上述本人认证消息的情况下，可向便携式终端120及计算机终端110中的1个以上传输上述本人认证消息。

[0117] 根据本发明的实施例，若从用户终端部100接收认证对应值eC，则验证密钥生成部332借助上述数学式5至数学式8来生成与上述认证对应值eC相对应的验证密钥C′。

[0118] 验证部335借助在上述验证密钥生成部332中生成的上述验证密钥C′执行对于上述认证对应值eC的验证，并向服务器200通知上述结果。当适用数学式8时，验证部335为与不用于验证密钥(C′)译码的一次性随机密钥K相对应的密钥K′。因此，当适用数学式8时，验证部335通过判断验证密钥C′和一次性随机密钥K是否相同来执行认证。

[0119] 在上述说明中，说明了上述本人认证服务器部300由1个服务器构成的情况，但是，在以短消息服务/长消息服务/多媒体消息服务消息的方式直接传输本人认证消息的情况下，上述消息处理部11可由移动通信消息发送服务器(未图示)构成，在从便携式终端120直接接受认证对应值的情况下，上述消息处理部11也可由应用服务器构成。

[0120] 图4为示出本发明第一实施例的利用移动通信消息及一次性随机密钥的本人确认及防盗用方法的流程图。

[0121] 参照图4，首先，用户终端部100与服务器200相连接之后(步骤S101)，借助需要本人认证的服务的选择来检查是否发生本人认证事件(步骤S103)。

[0122] 若发生本人认证事件，则用户终端部100从用户接收本人认证所需要的用户输入信息，并向服务器200传输包含上述用户输入信息的本人认证执行请求信号(步骤S105)。

[0123] 当请求执行认证时，服务器200向本人认证服务器部300传输包含上述用户输入信息的本人认证请求信号(步骤S107)，本人认证服务器部300向以往认证系统400传输上述认证请求信号来请求本人认证(步骤S109)。

[0124] 以往认证系统400对上述用户输入信息和与预先登录的上述用户输入信息的用户相对应的用户信息进行比较，由此判断是否相同(步骤S111)。

[0125] 当本人信息不同时，以往认证系统400向本人认证服务器部300传输包含本人认证不同通知消息的本人认证不同通知信号(步骤S113)，当本人信息相同时，向本人认证服务器部300传输通知本人信息相同信号(步骤S115)。

[0126] 本人认证服务器部300也判断从以往认证系统400接收的本人信息相同结果是否一致之后(步骤S117)之后，向服务器200传输本人确认结果信息(步骤S119、步骤S121)。

[0127] 服务器200判断本人认证结果信息是否相同(步骤S123)，若本人认证结果信息不同，则向用户终端部100通知本人信息不同(步骤S125)，若本人认证结果信息相同，则被设定为服务待机模式，直到接收本人认证结果(步骤S127)。

[0128] 收到本人信息相同的通报的本人认证服务器部300在通知上述本人认证相同之后(步骤S121)，对1个一次性随机密钥K或如上述数学式4所示，对不同的2个一次性随机密钥K、R1执行异或运算来生成认证密钥C(步骤S129)。

[0129] 若生成认证密钥C，则本人认证服务器部300向服务器200提供上述认证密钥C，来生成包含上述认证密钥C的本人认证消息，由此向用户终端部100的便携式终端120提供上述本人认证消息(步骤S131、步骤S133)。此时的本人认证消息能够以短消息服务/长消息服务/多媒体消息服务等的移动通信消息的方式传输。

[0130] 并且，本人认证服务器部300可直接以移动通信消息的形态向便携式终端120传输包括所生成的认证密钥C的本人认证消息(步骤S134)。

[0131] 并且，本人认证服务器部300向以往认证系统400提供认证密钥C，以往认证系统400生成包含上述认证密钥C的本人认证消息之后，可向对应用户终端部100的便携式终端120传输上述本人认证消息(步骤S135、步骤S137)。此时的本人认证消息也能够以移动通信消息的方式传输。接收本人认证消息的便携式终端120也可显示本人认证消息，为了提高安全，也可以不显示本人认证消息。

[0132] 若接收上述本人认证消息，则便携式终端120生成安全密钥R(步骤S138)。

[0133] 若生成上述安全密钥R，则便携式终端120对上述安全密钥R和上述认证密钥C适用

上述数学式1至数学式3中的1个来生成认证对应值eC(步骤S139)。

[0134] 若计算出上述认证对应值eC,则便携式终端120向本人认证服务器部300提供上述生成的安全密钥R(步骤S141)。

[0135] 在提供上述安全密钥R之后,便携式终端120可直接向本人认证服务器部300传输上述认证对应值eC(步骤S143),如图4中以虚线及长短划线所示,也可通过用户终端部100的计算机终端110(步骤S145、步骤S147、步骤S149、步骤S151)向本人认证服务器部300传输认证对应值eC。上述计算机终端110可直接向本人认证服务器部300传输认证对应值eC(步骤S145、步骤S151),也可通过服务器200传输认证对应值eC(步骤S145、步骤S147、步骤S149)。

[0136] 接收安全密钥R及认证对应值eC的本人认证服务器部300借助在上述数学式5至8中,与适用于生成上述认证对应值的上述数学式1至数学式4的1个相对应的数学式生成验证密钥C′(步骤S153)。

[0137] 若生成上述验证密钥C′,则本人认证服务器部300借助上述验证密钥C′验证上述认证对应值eC,由此判断是否验证成功(步骤S155)。

[0138] 判断结果,若失败,则本人认证服务器部300通知服务器200本人认证失败(步骤S157),若本人认证成功,则通知服务器200本人认证成功(步骤S159)。

[0139] 接收上述本人认证结果的服务器200接触上述服务待机模式,并向执行服务的用户终端部100的计算机终端110传输本人认证结果,且向上述计算机终端110提供对应服务(步骤S161)。

[0140] 并且,在提供上述验证结果之后,本人认证服务器部300可按用户及服务器200,将处理明细存储于存储部340(步骤S163)。

[0141] 并且,本人认证服服务器部300可向以往认证系统400传输上述认证处理明细(步骤S165)。

[0142] 图5为示出本发明第二实施例的利用移动通信消息及一次性随机密钥的本人认证及防盗用方法的流程图。图5中,与上述图4相同的步骤使用相同的标记,根据第二实施例,对不同结构使用不同标记。因此,在参照图5说明本发明的过程中,以上述不同结构为主进行说明。

[0143] 本人认证服务器部300向用户终端部100的便携式终端120传输包含认证密钥C的本人认证消息之后(步骤S131至步骤S133、步骤S134、步骤S135至步骤S137),生成安全密钥R(步骤S210),向便携式终端120提供所生成的安全密钥R(步骤S211)。

[0144] 根据实施例,接收上述安全密钥R的便携式终端120借助上述数学式1至数学式3中的1个对从本人认证服务器部300接收的认证密钥C和上述安全密钥R计算认证对应值eC(步骤S213)。

[0145] 若计算出认证对应值eC,则便携式终端120直接向安全认证服务器部300传输所计算的认证对应值eC(步骤S215)。

[0146] 并且,若显示计算出便携式终端120的认证对应值,则用户通过计算机终端110输入所显示的认证对应值eC(步骤S217),通过服务器200(步骤S219、步骤S221)或直接(步骤S223)向本人认证服务器部300传输所输入的认证对应值eC。

[0147] 接收认证对应值eC的本人认证服务器部300对接收的认证对应值eC和上述所生成

的安全密钥R适用与上述数学式5至数学式8中相对应的数学式来计算验证密钥C′(步骤S225)。

[0148] 若计算出验证密钥C′,则本人认证服务器部300及服务器200通过与上述图3相同的步骤执行基于认证结果的处理。

[0149] 图6为示出本发明第三实施例的利用二维码及一次性随机密钥的本人确认及防盗用方法的流程图。以下,在参照图6说明本发明的过程中,应留意的是,对与上述图4及图5相同步骤省略对其的说明,或者进行简单说明。

[0150] 在图6中,若生成认证密钥C,则本人认证服务器部300生成包含所生成的认证密钥C的本人认证消息(步骤S129)之后,生成包含所生成的本人认证消息的二维码(步骤S311)。

[0151] 若上述本人认证消息变换为二维码,则上述本人认证服务器部300向用户终端部100的计算机终端110及便携式终端120中的1个以上传输变换的二维码本人认证消息(步骤S313)。

[0152] 接受上述二维码本人认证消息的计算机终端110及便携式终端120可显示二维码本人认证消息(步骤S315)。

[0153] 在计算机终端110显示二维码的情况下,便携式终端120通过输入部30直接接受二维码的代码,或者通过扫描部60对二维码进行扫描并取得二维码之后,对认证密钥C进行检测(步骤S317)。

[0154] 若取得上述认证密钥C,则便携式终端120生成安全密钥R(步骤S318),对上述认证密钥C和所生成的安全密钥R适用上述数学式1至数学式3来生成认证对应值eC(步骤S319)。

[0155] 若生成上述认证对应值eC,则便携式终端120向本人认证服务器部300提供上述所生成的安全密钥R(步骤S321)。

[0156] 在传输上述安全密钥R之后,便携式终端120或计算机终端110向本人认证服务器300传输认证对应值eC(步骤S323、步骤S325至步骤S329、步骤S331)。

[0157] 根据情况,上述安全密钥R和认证对应值eC能够以构成为1个消息形态的方式被一同传输。

[0158] 接收安全密钥R及认证对应值eC的本人认证服务器部300借助上述数学式5至数学式8中相对应的1个数学式对验证密钥C′计算之后(步骤S333)之后,执行基于所生成的验证密钥C′的验证(步骤S155)。与上述图4及图5相同的之后的过程与图4相同,因此将省略对其的说明。

[0159] 图7为示出本发明第四实施例的利用二维码及一次性随机密钥的本人确认及防盗用方法的流程图。

[0160] 参照图7,与图6相同,若本人认证服务器部300以二维码形态向用户终端部100的计算机终端110及便携式终端120中的1个以上传输包含认证密钥的本人认证消息(步骤S313),则接收上述二维码的上述计算机终端110及便携式终端120在画面显示二维码(步骤S315)。

[0161] 在传送上述二维码之后,本人认证服务器部300在生成安全密钥R之后(步骤S410),向用户终端100的便携式终端120传输上述安全密钥R(步骤S411)。

[0162] 在计算机终端110显示上述二维码的情况下,便携式终端120通过输入部30直接接受二维码的代码,或者通过扫描部60对二维码进行扫描并取得二维码之后,对认证密钥C进

行检测(步骤S413)。

[0163] 若取得上述认证密钥C,则便携式终端120对从上述本人认证服务器部300接收的安全密钥R和上述认证密钥C适用上述数学式1至数学式3来生成认证对应值eC(步骤S415)。

[0164] 若生成上述认证对应值eC,则便携式终端120或计算机终端110向本人认证服务器300传输认证对应值eC(步骤S417、步骤S419至步骤S425、步骤S419及步骤S427)。

[0165] 接收认证对应值eC的本人认证服务器部300借助与上述数学式5至8中相对应的1个数学式计算验证密钥C′(步骤S429)之后,执行基于所生成的验证密钥C′的验证(步骤S155)。

[0166] 另一方面,本发明并不局限于上述典型的优选实施例,本发明所属技术领域的普通技术人员容易理解可在不超出本发明的主旨的范围内进行多种改良、变更、代替或附加。只要基于上述改良、变更、代替或附加的实施属于发明要求保护范围的范畴,则其技术思想也属于本发明。

[0167] 附图标记的说明

[0168] 10:便携式终端控制部 11:消息处理部

[0169] 12:认证密钥取得部 13:认证对应值生成部

[0170] 20:存储部 30:输入部

[0171] 40:显示部 50:通信部

[0172] 60:扫描部 100:用户终端部

[0173] 110:计算机终端 120:便携式终端

[0174] 200:服务器 300:本人认证服务器部

[0175] 310:认证控制部 320:用户登录部

[0176] 330:认证处理部 331:本人认证消息生成部

[0177] 332:验证密钥生成部 333:验证部

[0178] 340:存储部 350:通信部

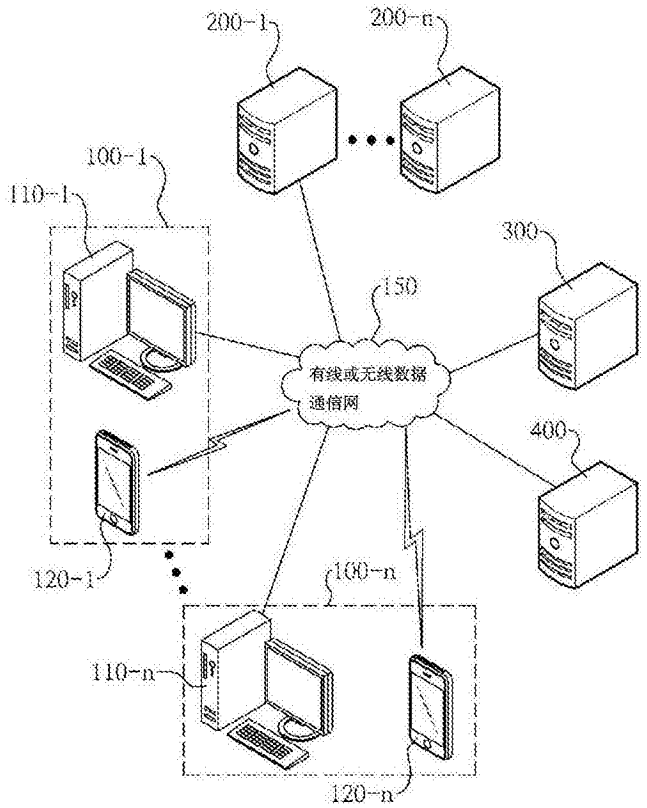

200-1
200-n
100-1
110-1
300
150
有线或无线数据通信网
400
120-1
100-n
110-n
120-n

图1

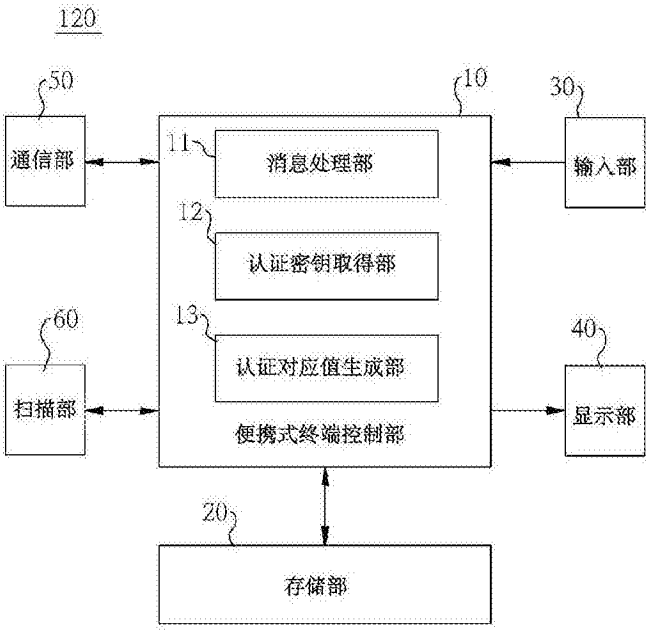

120
50
10
30
通信部
11
消息处理部
输入部
12
认证密钥取得部
60
13
40
扫描部
认证对应值生成部
显示部
便携式终端控制部
20
存储部

图2

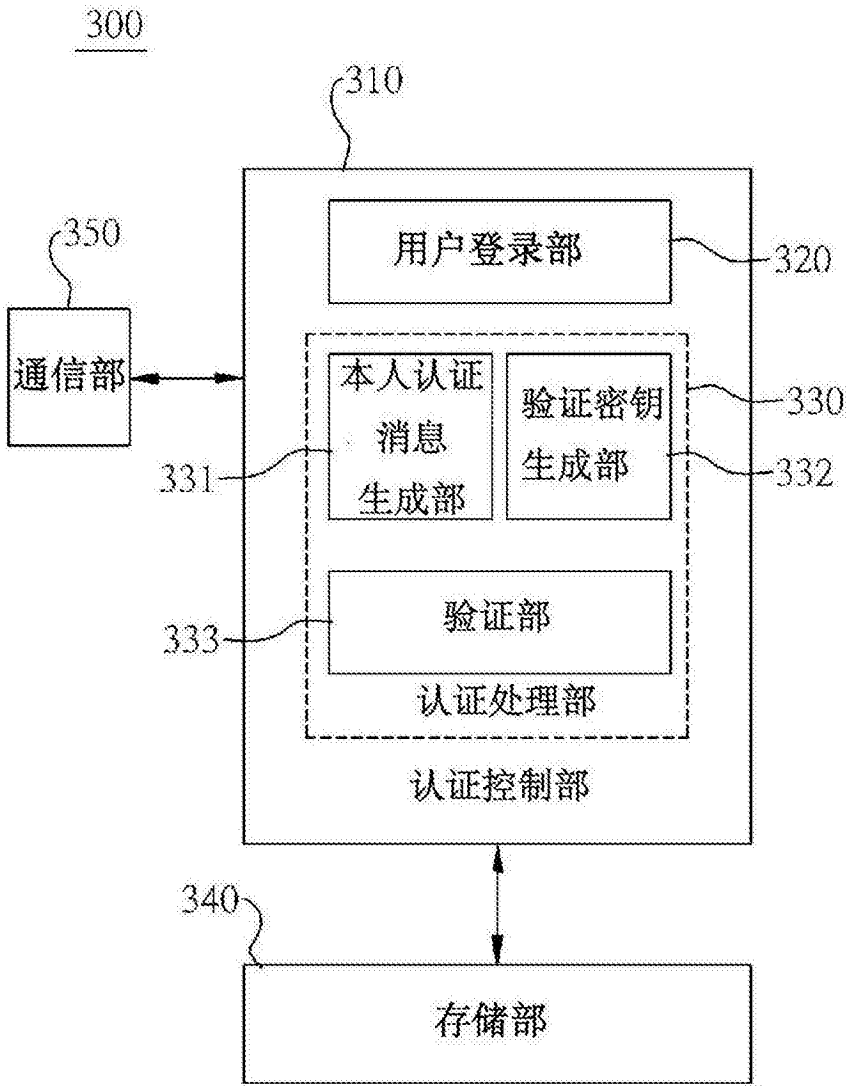

300
310
350
用户登录部
320
通信部
本人认证
消息
生成部
验证密钥
生成部
330
331
332
验证部
333
认证处理部
认证控制部
340
存储部

图3

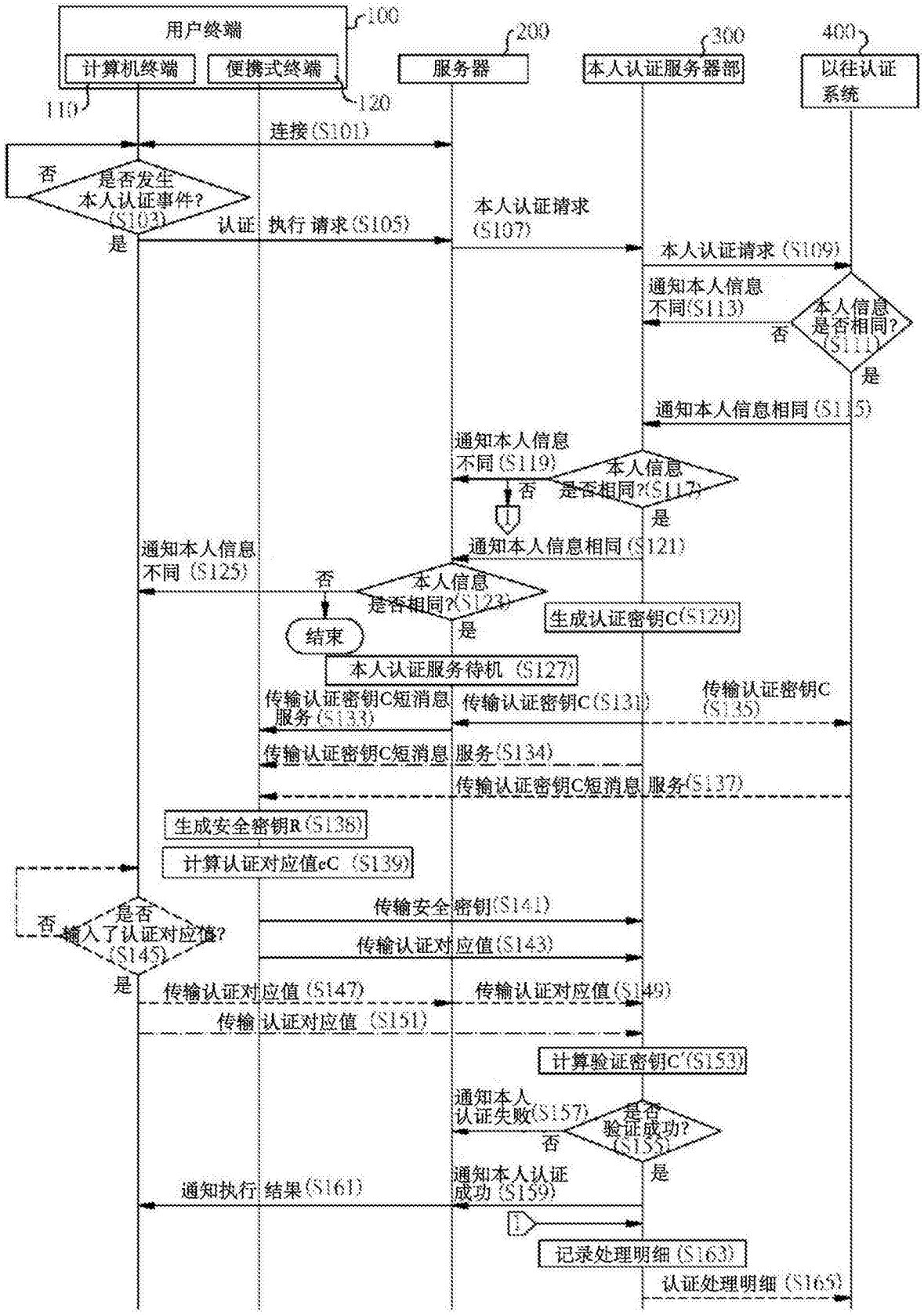

用户终端
100
计算机终端
便携式终端
110
120
服务器
200
本人认证服务器部
300
以往认证系统
400
连接(S101)
否
是否发生本人认证事件?(S103)
是
认证执行请求(S105)
本人认证请求(S107)
本人认证请求(S109)
通知本人信息不同(S113)
本人信息是否相同?(S111)
否
是
通知本人信息相同(S115)
通知本人信息不同(S119)
本人信息是否相同?(S117)
否
是
通知本人信息相同(S121)
通知本人信息不同(S125)
否
本人信息是否相同?(S123)
是
结束
生成认证密钥C(S129)
本人认证服务待机(S127)
传输认证密钥C短消息服务(S133)
传输认证密钥C(S131)
传输认证密钥C(S135)
传输认证密钥C短消息服务(S134)
传输认证密钥C短消息服务(S137)
生成安全密钥R(S138)
计算认证对应值eC(S139)
传输安全密钥(S141)
否
是否输入了认证对应值?(S145)
是
传输认证对应值(S143)
传输认证对应值(S147)
传输认证对应值(S149)
传输认证对应值(S151)
计算验证密钥C'(S153)
通知本人认证失败(S157)
是否验证成功?(S155)
否
是
通知执行结果(S161)
通知本人认证成功(S159)
记录处理明细(S163)
认证处理明细(S165)

图4

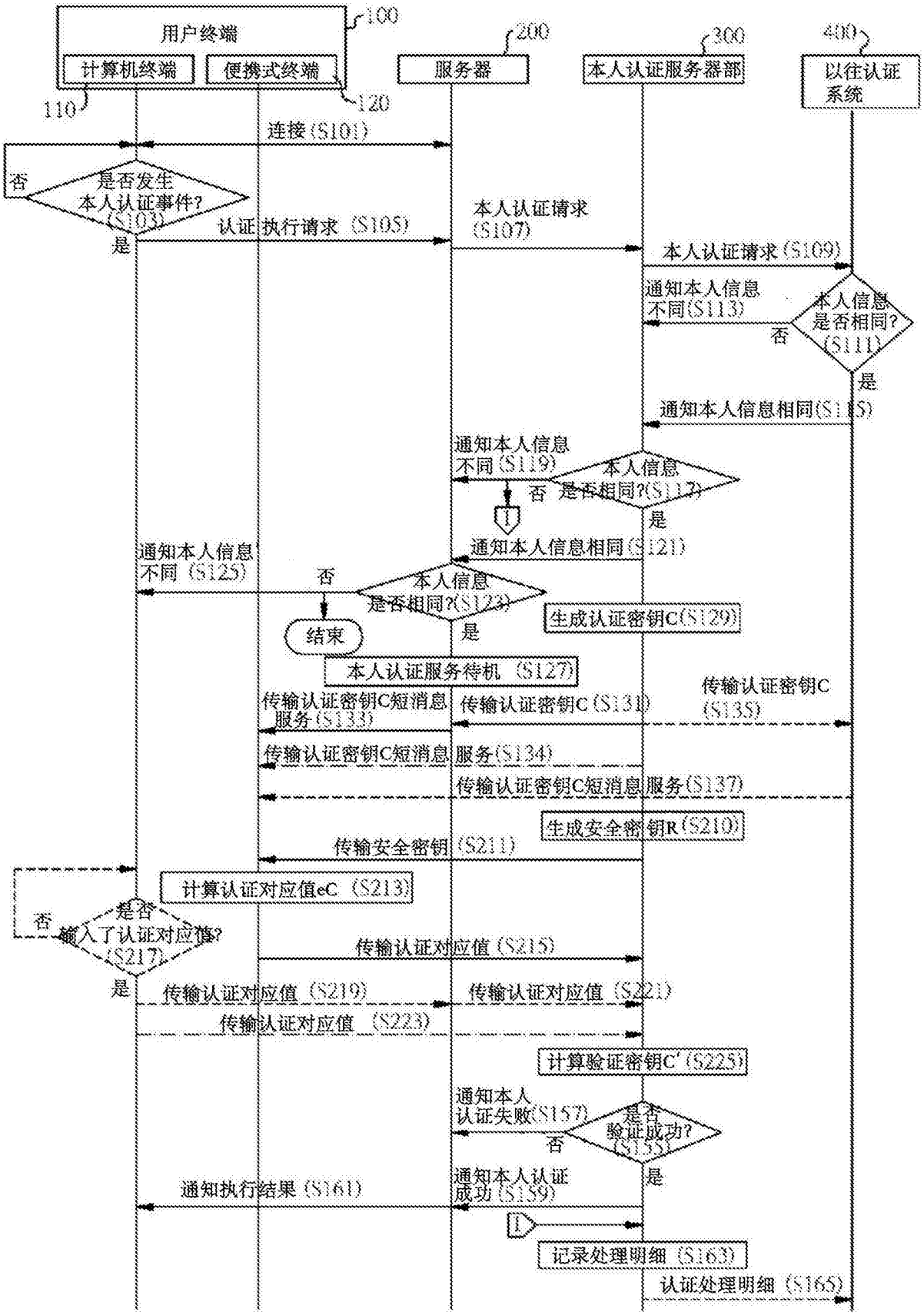

用户终端
100
计算机终端
便携式终端
110
120
服务器
200
本人认证服务器部
300
以往认证系统
400
连接(S101)
否
是否发生本人认证事件?(S103)
是
认证执行请求(S105)
本人认证请求(S107)
本人认证请求(S109)
通知本人信息不同(S113)
本人信息是否相同?(S111)
否
是
通知本人信息相同(S115)
通知本人信息不同(S119)
本人信息是否相同?(S117)
否
是
1
通知本人信息相同(S121)
通知本人信息不同(S125)
否
本人信息是否相同?(S123)
结束
是
生成认证密钥C(S129)
本人认证服务待机(S127)
传输认证密钥C短消息服务(S133)
传输认证密钥C(S131)
传输认证密钥C(S135)
传输认证密钥C短消息服务(S134)
传输认证密钥C短消息服务(S137)
生成安全密钥R(S210)
传输安全密钥(S211)
计算认证对应值eC(S213)
否
是否输入了认证对应值?(S217)
是
传输认证对应值(S215)
传输认证对应值(S219)
传输认证对应值(S221)
传输认证对应值(S223)
计算验证密钥C'(S225)
通知本人认证失败(S157)
是否验证成功?(S155)
否
是
通知本人认证成功(S159)
通知执行结果(S161)
1
记录处理明细(S163)
认证处理明细(S165)

图5

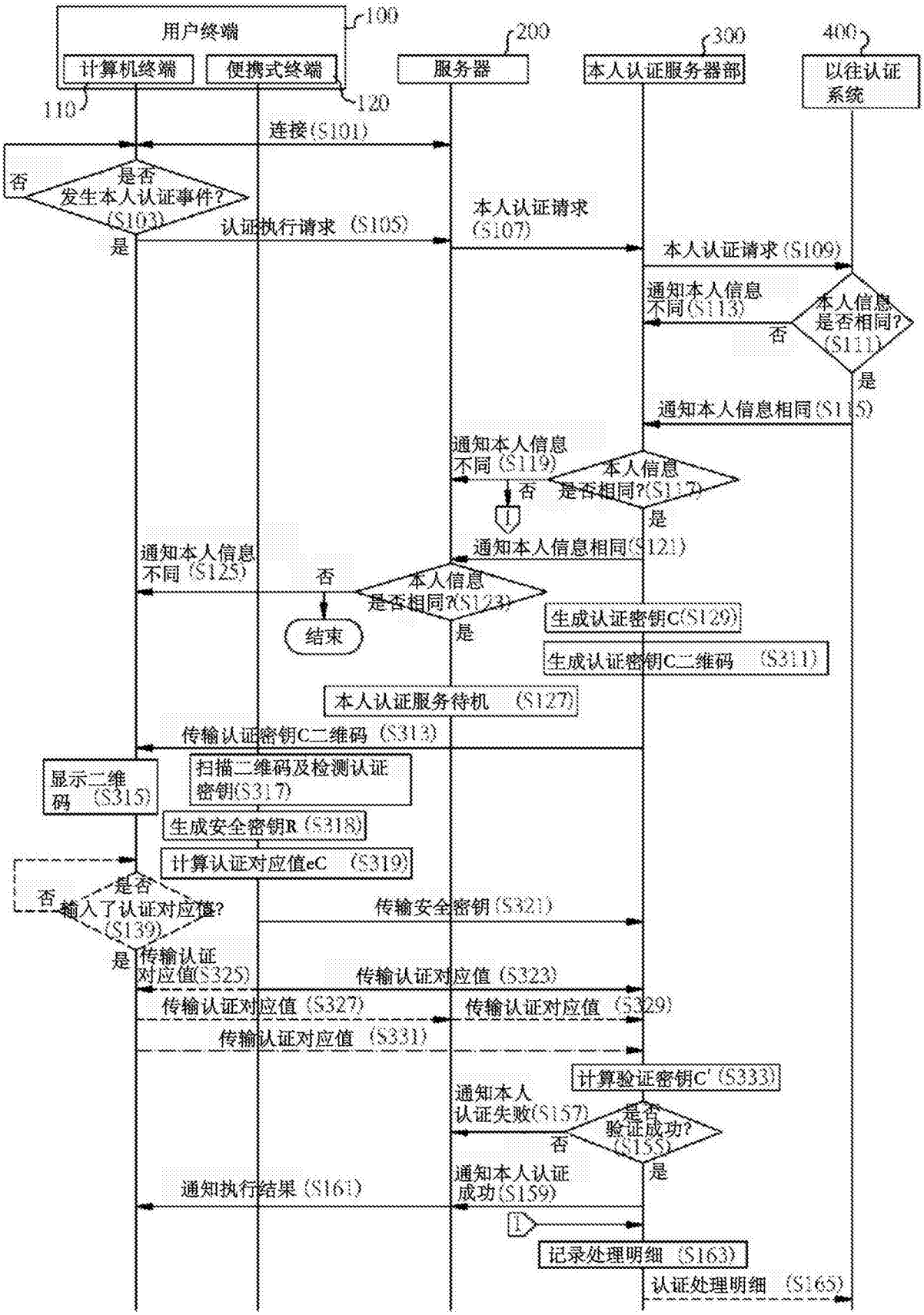

用户终端
100
计算机终端
便携式终端
110
120
服务器
200
本人认证服务器部
300
以往认证系统
400
连接(S101)
否
是否发生本人认证事件?(S103)
是
认证执行请求 (S105)
本人认证请求(S107)
本人认证请求(S109)
通知本人信息不同(S113)
本人信息是否相同?(S111)
否
是
通知本人信息相同(S115)
通知本人信息不同(S119)
本人信息是否相同?(S117)
否
是
通知本人信息相同(S121)
通知本人信息不同(S125)
否
本人信息是否相同?(S123)
结束
是
生成认证密钥C(S129)
生成认证密钥C二维码 (S311)
本人认证服务待机 (S127)
传输认证密钥C二维码 (S313)
显示二维码 (S315)
扫描二维码及检测认证密钥(S317)
生成安全密钥R (S318)
计算认证对应值eC (S319)
否
是否输入了认证对应值?(S139)
是
传输安全密钥 (S321)
传输认证对应值(S325)
传输认证对应值 (S323)
传输认证对应值 (S327)
传输认证对应值 (S329)
传输认证对应值 (S331)
计算验证密钥C' (S333)
通知本人认证失败(S157)
否
是否验证成功?(S155)
是
通知执行结果 (S161)
通知本人认证成功(S159)
记录处理明细 (S163)
认证处理明细 (S165)

图6

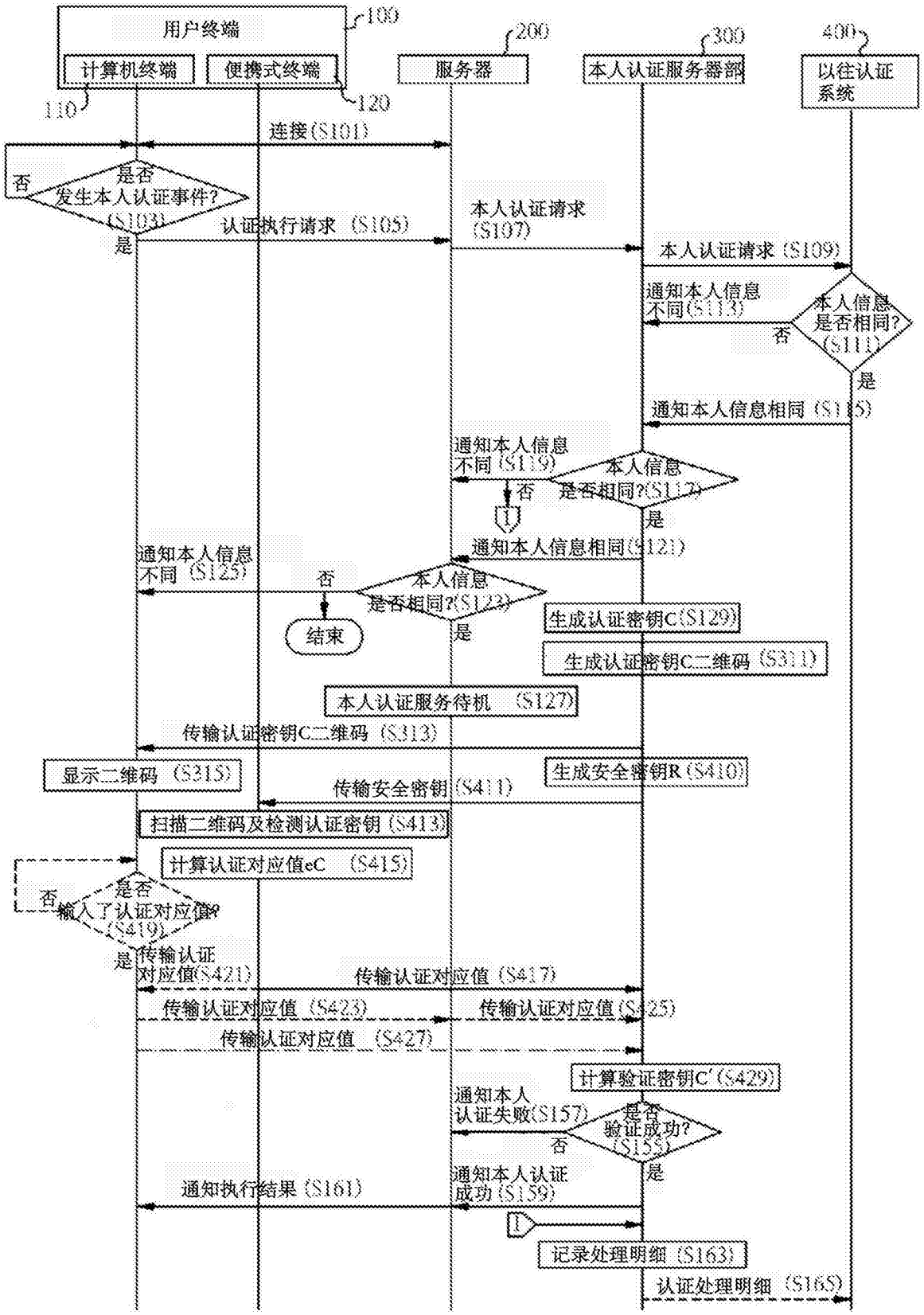

用户终端
100
计算机终端
便携式终端
110
120
服务器
200
本人认证服务器部
300
以往认证系统
400
连接(S101)
否
是否发生本人认证事件?(S103)
是
认证执行请求 (S105)
本人认证请求(S107)
本人认证请求 (S109)
通知本人信息不同(S113)
本人信息是否相同?(S111)
否
是
通知本人信息相同 (S115)
通知本人信息不同 (S119)
本人信息是否相同?(S117)
否
是
通知本人信息相同(S121)
通知本人信息不同 (S125)
否
本人信息是否相同?(S123)
结束
是
生成认证密钥C(S129)
生成认证密钥C二维码 (S311)
本人认证服务待机 (S127)
传输认证密钥C二维码 (S313)
显示二维码 (S315)
生成安全密钥R (S410)
传输安全密钥(S411)
扫描二维码及检测认证密钥 (S413)
计算认证对应值eC (S415)
否
是否输入了认证对应值?(S419)
是
传输认证对应值(S421)
传输认证对应值 (S417)
传输认证对应值 (S423)
传输认证对应值 (S425)
传输认证对应值 (S427)
计算验证密钥C' (S429)
通知本人认证失败(S157)
是否验证成功?(S155)
否
是
通知本人认证成功(S159)
通知执行结果 (S161)
记录处理明细 (S163)
认证处理明细 (S165)

图7