(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 111709803 A
(43)申请公布日 2020.09.25

(21)申请号 202010536534.1

(22)申请日 2020.06.12

(71)申请人 北京思特奇信息技术股份有限公司
地址 100089 北京市海淀区中关村南大街6号中电信息大厦16层

(72)发明人 赵东伟

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 厉洋洋

(51)Int.Cl.
G06Q 30/06(2012.01)
G06Q 50/32(2012.01)

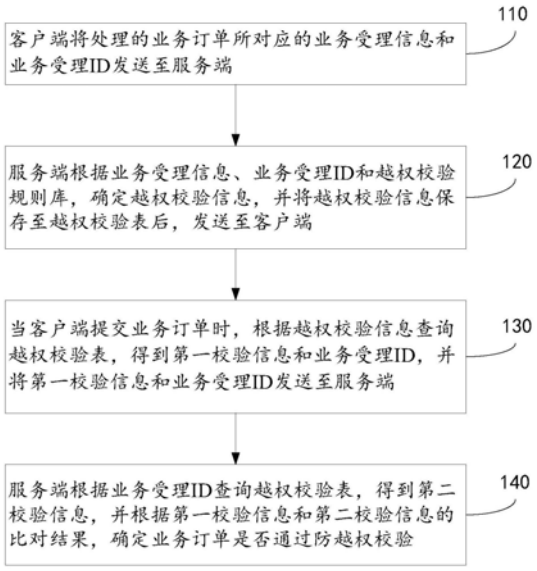
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种防止越权办理业务的方法和系统

(57)摘要

本发明涉及提供一种防止越权办理业务的方法和系统，包括客户端将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端；服务端根据业务受理信息、业务受理ID和越权校验规则库，确定越权校验信息，并将越权校验信息保存至越权校验表后，发送越权校验信息至客户端；当客户端提交业务订单时，根据越权校验信息查询越权校验表，得到第一校验信息和业务受理ID，并将第一校验信息和业务受理ID发送至服务端；服务端根据业务受理ID查询越权校验表，得到第二校验信息，并根据第一校验信息和第二校验信息的比对结果，确定业务订单是否通过防越权校验。本发明提出了一种防越权攻击的方法，不依赖加解密也可以防越权攻击。



CN 111709803 A

1.一种防止越权办理业务的方法,其特征在于,所述方法包括:

客户端将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端;

所述服务端根据所述业务受理信息、所述业务受理ID和越权校验规则库,确定越权校验信息,并将所述越权校验信息保存至越权校验表后,发送所述越权校验信息至所述客户端;

当所述客户端提交所述业务订单时,根据所述越权校验信息查询所述越权校验表,得到第一校验信息和所述业务受理ID,并将所述第一校验信息和所述业务受理ID发送至服务端;

所述服务端根据所述业务受理ID查询所述越权校验表,得到第二校验信息,并根据所述第一校验信息和所述第二校验信息的比对结果,确定所述业务订单是否通过防越权校验。

2.根据权利要求1所述的防止越权办理业务的方法,其特征在于,所述服务端根据所述业务受理信息、所述业务受理ID和越权校验规则库,确定越权校验信息,具体包括:

根据所述业务受理信息查询所述越权校验规则库,确定越权校验规则;

根据所述越权校验规则,从所述业务受理信息中筛选出预越权校验信息;

组合所述预越权校验信息和所述业务受理ID,得到所述越权校验信息。

3.根据权利要求1所述的防止越权办理业务的方法,其特征在于,所述服务端根据所述第一校验信息和所述第二校验信息的比对结果,确定所述业务订单是否通过防越权校验,具体包括:

所述服务端将所述第一校验信息和所述第二校验信息进行比对;

当所述第一校验信息和所述第二校验信息一致时,确定所述业务订单通过防越权校验;

否则,所述业务订单未通过防越权校验。

4.根据权利要求1所述的防止越权办理业务的方法,其特征在于,所述客户端将业务受理信息和业务受理ID发送至服务端之前,还包括:

客户端获取业务订单对应的业务受理信息,并根据所述业务受理信息生成业务受理ID。

5.根据权利要求1-4中任一项所述的防止越权办理业务的方法,其特征在于,所述业务受理信息包括办理所述业务订单的工作人员信息、客户信息和所述业务订单的信息。

6.一种防止越权办理业务的系统,其特征在于,包括客户端和服务端,

所述客户端,用于将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端;

所述服务端,用于根据所述业务受理信息、所述业务受理ID和越权校验规则库,确定越权校验信息,并将所述越权校验信息保存至越权校验表后,发送所述越权校验信息至所述客户端;

所述客户端,用于当提交所述业务订单时,根据所述越权校验信息查询所述越权校验表,得到第一校验信息和所述业务受理ID,并将所述第一校验信息和所述业务受理ID发送至服务端;

所述服务端,用于根据所述业务受理ID查询所述越权校验表,得到第二校验信息,并根

据所述第一校验信息和所述第二校验信息的比对结果，确定所述业务订单是否通过防越权校验。

7.根据权利要求6所述的防止越权办理业务的系统，其特征在于：

所述服务端，具体用于根据所述业务受理信息查询所述越权校验规则库，确定越权校验规则；

根据所述越权校验规则，从所述业务受理信息中筛选出预越权校验信息；

组合所述预越权校验信息和所述业务受理ID，得到所述越权校验信息。

8.根据权利要求6所述的防止越权办理业务的系统，其特征在于：

所述服务端，具体用于将所述第一校验信息和所述第二校验信息进行比对；

当所述第一校验信息和所述第二校验信息一致时，确定所述业务订单通过防越权校验；

否则，所述业务订单未通过防越权校验。

9.根据权利要求6所述的防止越权办理业务的系统，其特征在于，

所述客户单，还用于获取业务订单对应的业务受理信息，并根据所述业务受理信息生成业务受理ID。

10.根据权利要求6-9中任一项所述的防止越权办理业务的系统，其特征在于，所述业务受理信息包括办理所述业务订单的工作人员信息、客户信息和所述业务订单的信息。

一种防止越权办理业务的方法和系统

技术领域

[0001] 本发明涉及电信业务技术领域,尤其涉及一种防止越权办理业务的方法和系统。

背景技术

[0002] 电信行业CRM系统为国内比较复杂的IT支撑系统,在安全防护方面有其自身的特点和需求。

[0003] 在目前的电信CRM系统中,传统的工作人员受理页面与订单中心的后台由于处于电信系统的企业专网,目前前后台的数据传输没有采用报文加密等的技术手段。一些代理商合作伙伴也通过VPN连接到电信的企业专网,营业受理页面同样也会给代理商的工作人员使用。在这种特定的背景下,一旦存在恶意的技术人员截获了订单中心的订单创建报文,就能够通过修改参数的技术手段,通过恶意程序调用订单中心的订单创建服务来达到其非法办理业务的目的。

发明内容

[0004] 本发明所要解决的技术问题是针对现有技术的不足,提供一种防止越权办理业务的方法和系统。

[0005] 本发明解决上述技术问题的技术方案如下:

[0006] 一种防止越权办理业务的方法,所述方法包括:

[0007] 客户端将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端;

[0008] 所述服务端根据所述业务受理信息、所述业务受理ID和越权校验规则库,确定越权校验信息,并将所述越权校验信息保存至越权校验表后,发送所述越权校验信息至所述客户端;

[0009] 当所述客户端提交所述业务订单时,根据所述越权校验信息查询所述越权校验表,得到第一校验信息和所述业务受理ID,并将所述第一校验信息和所述业务受理ID发送至服务端;

[0010] 所述服务端根据所述业务受理ID查询所述越权校验表,得到第二校验信息,并根据所述第一校验信息和所述第二校验信息的比对结果,确定所述业务订单是否通过防越权校验。

[0011] 本发明的有益效果是:提供一种防止越权办理业务的方法,包括客户端将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端,服务端根据业务受理信息、业务受理ID和越权校验规则库,确定越权校验信息,并将越权校验信息保存至越权校验表后,发送至客户端;当客户端提交业务订单时,根据越权校验信息查询越权校验表,得到第一校验信息和业务受理ID,并将第一校验信息和业务受理ID发送至服务端;服务端根据业务受理ID查询越权校验表,得到第二校验信息,并根据第一校验信息和第二校验信息的比对结果,确定业务订单是否通过防越权校验。本发明提出了一种防越权攻击的方法,不依赖加解密也可以防越权攻击。

[0012] 在上述技术方案的基础上，本发明还可以做如下改进。

[0013] 进一步地，所述服务端根据所述业务受理信息、所述业务受理ID和越权校验规则库，确定越权校验信息，具体包括：

[0014] 根据所述业务受理信息查询所述越权校验规则库，确定越权校验规则；

[0015] 根据所述越权校验规则，从所述业务受理信息中筛选出预越权校验信息；

[0016] 组合所述预越权校验信息和所述业务受理ID，得到所述越权校验信息。

[0017] 采用上述进一步方案的有益效果是：根据业务受理信息，确定越权校验信息，可灵活定制越权校验信息，提升防越权攻击能力。

[0018] 进一步地，所述服务端根据所述第一校验信息和所述第二校验信息的比对结果，确定所述业务订单是否通过防越权校验，具体包括：

[0019] 所述服务端将所述第一校验信息和所述第二校验信息进行比对；

[0020] 当所述第一校验信息和所述第二校验信息一致时，确定所述业务订单通过防越权校验；

[0021] 否则，所述业务订单未通过防越权校验。

[0022] 进一步地，所述客户端将业务受理信息和业务受理ID发送至服务端之前，还包括：

[0023] 客户端获取业务订单对应的业务受理信息，并根据所述业务受理信息生成业务受理ID。

[0024] 进一步地，所述业务受理信息包括办理所述业务订单的工作人员信息、客户信息和所述业务订单的信息。

[0025] 本发明解决上述技术问题的另一种技术方案如下：

[0026] 一种防止越权办理业务的系统，包括客户端和服务端，

[0027] 所述客户端，用于将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端；

[0028] 所述服务端，用于根据所述业务受理信息、所述业务受理ID和越权校验规则库，确定越权校验信息，并将所述越权校验信息保存至越权校验表后，发送所述越权校验信息至所述客户端；

[0029] 所述客户端，用于当提交所述业务订单时，根据所述越权校验信息查询所述越权校验表，得到第一校验信息和所述业务受理ID，并将所述第一校验信息和所述业务受理ID发送至服务端；

[0030] 所述服务端，用于根据所述业务受理ID查询所述越权校验表，得到第二校验信息，并根据所述第一校验信息和所述第二校验信息的比对结果，确定所述业务订单是否通过防越权校验。

[0031] 本发明的有益效果是：提供一种防止越权办理业务的系统，包括客户端，用于将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端，服务端根据业务受理信息、业务受理ID和越权校验规则库，确定越权校验信息，并将越权校验信息保存至越权校验表后，发送至客户端；当客户端提交业务订单时，根据越权校验信息查询越权校验表，得到第一校验信息和业务受理ID，并将第一校验信息和业务受理ID发送至服务端；服务端根据业务受理ID查询越权校验表，得到第二校验信息，并根据第一校验信息和第二校验信息的比对结果，确定业务订单是否通过防越权校验。本发明提出了一种防越权攻击的系统，并且

不依赖加解密也可以防越权攻击。

[0032] 在上述技术方案的基础上，本发明还可以做如下改进。

[0033] 进一步地，所述服务端，具体用于根据所述业务受理信息查询所述越权校验规则库，确定越权校验规则；

[0034] 根据所述越权校验规则，从所述业务受理信息中筛选出预越权校验信息；

[0035] 组合所述预越权校验信息和所述业务受理ID，得到所述越权校验信息。

[0036] 进一步地，所述服务端，具体用于将所述第一校验信息和所述第二校验信息进行比对；

[0037] 当所述第一校验信息和所述第二校验信息一致时，确定所述业务订单通过防越权校验；

[0038] 否则，所述业务订单未通过防越权校验。

[0039] 进一步地，所述客户单，还用于获取业务订单对应的业务受理信息，并根据所述业务受理信息生成业务受理ID。

[0040] 进一步地，所述业务受理信息包括办理所述业务订单的工作人员信息、客户信息和所述业务订单的信息。

[0041] 本发明附加的方面的优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明实践了解到。

附图说明

[0042] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面所描述的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0043] 图1为本发明实施例所述的一种防止越权办理业务的方法的流程示意图；

[0044] 图2为本发明实施例所述的一种防止越权办理业务的系统的架构图。

具体实施方式

[0045] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明的一部分实施例，而不是全部实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都应属于本发明保护的范围。

[0046] 如图1本发明实施例所述的一种防止越权办理业务的方法的流程示意图所示，一种防止越权办理业务的方法包括以下步骤：

[0047] 110、客户端将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端。

[0048] 120、服务端根据业务受理信息、业务受理ID和越权校验规则库，确定越权校验信息，并将越权校验信息保存至越权校验表后，发送越权校验信息至客户端。

[0049] 130、当客户端提交业务订单时，根据越权校验信息查询越权校验表，得到第一校验信息和业务受理ID，并将第一校验信息和业务受理ID发送至服务端。

[0050] 140、服务端根据业务受理ID查询越权校验表，得到第二校验信息，并根据第一校验信息和第二校验信息的比对结果，确定业务订单是否通过防越权校验。

[0051] 应理解，客户端可以是营业厅的工作人员的终端或是其他的设备，服务端可以是配置有订单中心的服务器，其中越权校验表可以保存在数据库中，可以是单独的数据库服务器或是订单中心服务器中的数据库。

[0052] 基于本实施例提供的提供一种防止越权办理业务的方法，包括客户端将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端，服务端根据业务受理信息、业务受理ID和越权校验规则库，确定越权校验信息，并将越权校验信息保存至越权校验表后，发送至客户端；当客户端提交业务订单时，根据越权校验信息查询越权校验表，得到第一校验信息和业务受理ID，并将第一校验信息和业务受理ID发送至服务端；服务端根据业务受理ID查询越权校验表，得到第二校验信息，并根据第一校验信息和第二校验信息的比对结果，确定业务订单是否通过防越权校验。本发明提出了一种防越权攻击的方法，不依赖加解密也可以防越权攻击。

[0053] 进一步地，所述服务端根据所述业务受理信息、所述业务受理ID和越权校验规则库，确定越权校验信息，具体包括：

[0054] 根据所述业务受理信息查询所述越权校验规则库，确定越权校验规则；

[0055] 根据所述越权校验规则，从所述业务受理信息中筛选出预越权校验信息；

[0056] 组合所述预越权校验信息和所述业务受理ID，得到所述越权校验信息。

[0057] 进一步地，所述服务端根据所述第一校验信息和所述第二校验信息的比对结果，确定所述业务订单是否通过防越权校验，具体包括：

[0058] 所述服务端将所述第一校验信息和所述第二校验信息进行比对；

[0059] 当所述第一校验信息和所述第二校验信息一致时，确定所述业务订单通过防越权校验；

[0060] 否则，所述业务订单未通过防越权校验。

[0061] 进一步地，所述客户端将业务受理信息和业务受理ID发送至服务端之前，还包括：

[0062] 客户端获取业务订单对应的业务受理信息，并根据所述业务受理信息生成业务受理ID。

[0063] 进一步地，所述业务受理信息包括办理所述业务订单的工作人员信息、客户信息和所述业务订单的信息。

[0064] 应理解，例如，当客户需要办理业务时，工作人员登录电信CRM受理页面，输入要办理业务的手机号码，获取业务受理信息，并根据业务受理信息生成业务受理ID，业务受理ID是作为此业务订单的唯一标识，将业务受理信息传递给订单中心。业务受理信息包括工作人员的基本信息，进行业务办理的用户信息。订单中心从数据库中读取越权校验规则，按照越权校验规则将业务受理ID以及业务受理信息中选取部分信息进行记录，形成越权校验信息，其中，业务受理信息部分信息的选择取决于越权校验规则，不同的规则所选取的信息不同。

[0065] 当工作人员对办理业务所需要的信息填写完毕，进行订单提交时，根据越权校验信息，查询越权校验表，得到第一校验信息和业务受理ID，将第一校验信息、业务受理ID和业务订单信息发送至订单中心。

[0066] 订单中心解析第一校验信息、业务受理ID,然后通过业务受理ID在越权校验表中查询,得到第二校验信息,将第一校验信息和第二校验信息进行比对,如果数据一致,则防越权校验通过,可以生成订单进行业务受理,如果数据不一致或者从表中查询不到数据,则防越权校验失败,不会进行订单创建。其中,越权校验规则表可在订单中心或其他存储设备存储,其包含的字段包括“业务受理ID”、“业务代码”和“规则明细”。通过“业务代码”字段可以控制防越权校验的粒度,通过“开关”可以控制防越权的生效和失效规则。

[0067] 如图2为本发明实施例所述的一种防止越权办理业务的系统的架构图所示,一种防止越权办理业务的系统,包括客户端和服务端,

[0068] 所述客户端,用于将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端;

[0069] 所述服务端,用于根据所述业务受理信息、所述业务受理ID和越权校验规则库,确定越权校验信息,并将所述越权校验信息保存至越权校验表后,发送所述越权校验信息至所述客户端;

[0070] 所述客户端,用于当提交所述业务订单时,根据所述越权校验信息查询所述越权校验表,得到第一校验信息和所述业务受理ID,并将所述第一校验信息和所述业务受理ID发送至服务端;

[0071] 所述服务端,用于根据所述业务受理ID查询所述越权校验表,得到第二校验信息,并根据所述第一校验信息和所述第二校验信息的比对结果,确定所述业务订单是否通过防越权校验。

[0072] 进一步地,所述服务端,具体用于根据所述业务受理信息查询所述越权校验规则库,确定越权校验规则;

[0073] 根据所述越权校验规则,从所述业务受理信息中筛选出预越权校验信息;

[0074] 组合所述预越权校验信息和所述业务受理ID,得到所述越权校验信息。

[0075] 进一步地,所述服务端,具体用于将所述第一校验信息和所述第二校验信息进行比对;

[0076] 当所述第一校验信息和所述第二校验信息一致时,确定所述业务订单通过防越权校验;

[0077] 否则,所述业务订单未通过防越权校验。

[0078] 进一步地,所述客户单,还用于获取业务订单对应的业务受理信息,并根据所述业务受理信息生成业务受理ID。

[0079] 进一步地,所述业务受理信息包括办理所述业务订单的工作人员信息、客户信息和所述业务订单的信息。

[0080] 以上,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到各种等效的修改或替换,这些修改或替换都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以权利要求的保护范围为准。

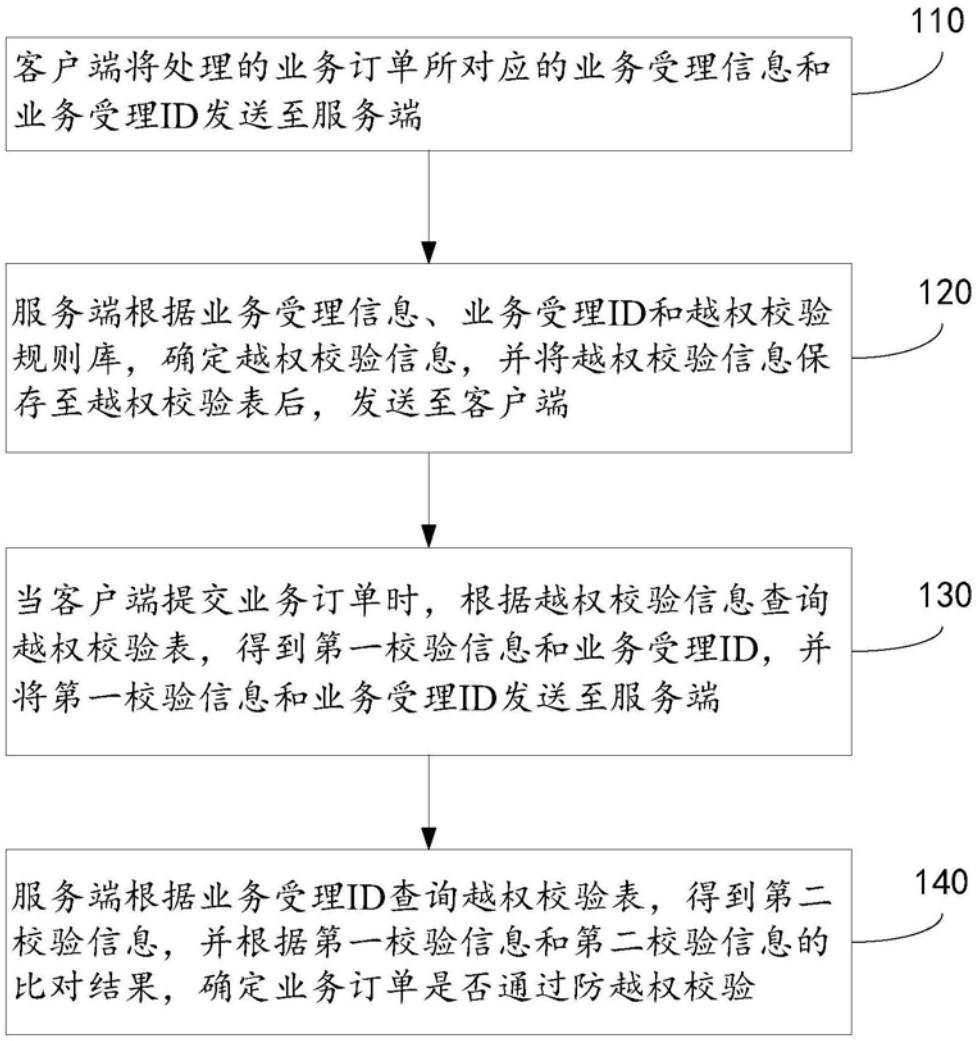

110
客户端将处理的业务订单所对应的业务受理信息和业务受理ID发送至服务端
120
服务端根据业务受理信息、业务受理ID和越权校验规则库，确定越权校验信息，并将越权校验信息保存至越权校验表后，发送至客户端
130
当客户端提交业务订单时，根据越权校验信息查询越权校验表，得到第一校验信息和业务受理ID，并将第一校验信息和业务受理ID发送至服务端
140
服务端根据业务受理ID查询越权校验表，得到第二校验信息，并根据第一校验信息和第二校验信息的比对结果，确定业务订单是否通过防越权校验

图1

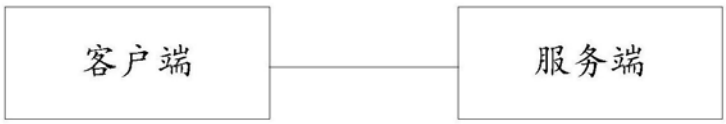

客户端
服务端

图2