产业链协同SaaS平台业务流程定制安全技术研究

曹 帅 王淑营
(西南交通大学CAD工程中心 成都 610031)

摘 要 针对产业链协同SaaS平台企业群以盟主企业为核心的业务流定制过程中的流程规则编排、存储/访问以及执行控制3个环节可能存在的安全隐患,建立了基于数字签名及业务实例关联的业务流程安全控制模型,对XML数字签名和验证模式、存储策略及模型执行策略进行了研究,提出了基于用户身份认证和业务实例关联的安全签名、存储和执行算法。对该安全模型和算法在汽车产业链协同SaaS平台企业群车辆售后的三包业务流程定制和执行过程进行了验证,结果表明其能防止业务流程在编排、存储和执行过程中被非法篡改和调用。

关键词 SaaS平台,安全,流程定制,数字签名
中图法分类号 TP393.0 **文献标识码** A

Research on Security Technology of Workflow Customization for Collaborative SaaS Platform of Industrial Chains

CAO Shuai WANG Shu-ying
(CAD Engineering Centre, Southwest Jiaotong University, Chengdu 610031, China)

Abstract A workflow control security model for security risks that may exist in the process of workflow rules choreography, storage/access and execution control in the workflow customization of collaborative SaaS platform of industrial chains with dominant enterprise as core was proposed based on the digital signature and service instance association. According to the research on the XML digital signature alone with its validating procedure and the strategy on storage and executing models, a digital signature which includes methods of validating the identity of users and is related to business operations, way of storing and arithmetic was proposed. The security model and arithmetic were validated in the customization and execution of the after service of vehicle on the collaborative SaaS platform of industrial chains, showing that it can prevent illegal tampering and transferring of workflow in the process of choreography, storage and execution.

Keywords SaaS platform, Security, Workflow customization, Digital signature

随着互联网的迅猛发展,SaaS充分利用网络技术与资源共享的特性,成为信息服务产业的主流[1]。SaaS以同一套软件多个应用实例为用户提供服务,以达到最大的共享,使软件成本和维护成本降到最低。而产业链协同SaaS平台是一个应用环境复杂、需求动态变化、用户类型众多、对可配置性和扩展性要求很高的复杂系统。其目标是为产业链企业群协作提供支撑,各企业联盟在应用过程中可以通过简单的配置和少量定制就可以通过平台实现协作。为满足用户在应用过程中对业务流程的个性化配置需求,笔者所在团队前期提出了SaaS平台面向多企业群的业务流程定制模型、业务流程驱动规则和加载控制方法,但该模型和算法缺乏对流程定制和执行过程中的安全技术的研究,特别是对基于Internet运行的为企业群提供零部件采购、产品销售和售后服务业务协同的SaaS平台而言,业务流程定制和执行过程中的安全性显得尤为重要,流程定制及控制过程中出现的任何安全问题都可能导致企业业务的混乱,给企业造成重大损失。

近年来,SaaS软件的个性化定制[2-5]已成为当前软件领域研究的热点。文献[6,7]在建立了流程定制模型的基础上,分别提出了基于应用的业务规则约束设计算法和将有向图转化为Petri网并运用Petri网的分析技术来验证全局定制行为的正确性的方法,有效地提高了租户的定制效率,但其只关注定制的流程本身是否正确、合理,未对流程定制过程中的安全性进行分析和解决。目前关于平台上不同企业群进行流程定制的安全性问题的研究较少。国外,Stormer H等人[8]建立了工作流安全模型,但并不适合SaaS平台面向对租户的特点。国内,琚洁慧[9]等人提出了SaaS的多租户实现方法并从技术和非技术两方面分析SaaS的安全技术;文献[10]从数据安全、网络安全和访问安全对基于SaaS的物流信息系统的安全现状进行分析并提出相应的解决对策,但均未分析和解决平台上业务的配置性和扩展性带来的安全问题;文献[11]提出了面向OA系统的工作流动态变化的引擎的研究并提出基于角色的权限控制解决访问安全问题,但由于产业链协同

到稿日期:2013-04-01 返修日期:2013-06-17 本文受国家科技支撑计划课题(2011BAH21B02,2011BAH21B03),四川省科技攻关技术项目(2010GZ0189),制造业产业链协同与信息化支撑技术四川省重点实验室开放项目(2013-002)资助。

曹 帅(1988—),女,硕士生;王淑营(1974—),女,博士,研究员,主要研究方向为基于SaaS平台的企业群业务协同技术。

SaaS平台面向多个企业群的不同角色，因此该方法不能解决其访问安全问题。

本文在上述研究的基础上，针对SaaS平台上流程定制中存在的安全隐患，建立了相应的安全控制模型及实现的关键技术。

1 产业链协同SaaS平台业务流程定制中的安全需求

1.1 产业链协同SaaS平台业务流程定制方案

产业链协同SaaS平台上的流程定制如图1所示。针对产业链协同SaaS平台对以不同龙头企业为核心的企业群个性化业务流程定制的支持，我们在前期对SaaS平台业务流程定制涉及的对象进行了定义和描述，包括SaaS平台的使用对象（即企业联盟）、SaaS平台为各企业群提供的业务、各企业群定制的流程模型以及流程实例，并建立了这些对象之间的关系模型即业务流程定制过程模型。根据产业链协同SaaS平台上业务流程的特点，在建立的模型基础上提出了该模型的驱动规则，包括顺序规则、分支规则、并发规则、抑或规则、聚合规则、异步参考规则。企业群业务流程定制实现的关键技术包括流程模型的存储、调用和加载，如图1所示。

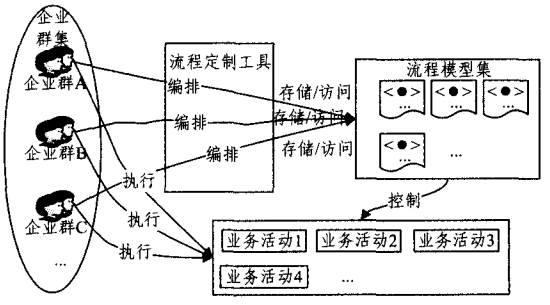


图1 产业链协同SaaS平台上的流程定制模型

1.2 SaaS平台业务流程定制模型中的安全需求

由图1所示的流程定制模型可看出，其整个过程包括编排→存储/访问→执行和控制，在以上3个环节中，若业务流程规则被篡改、非法访问或调用都将给平台带来一定的安全隐患，具体分析如下。

（1）业务流程编排过程中的安全需求：在编排活动中，各企业群的业务流程只能由本企业群的龙头企业进行编排，平台根据各龙头企业编排的流程模型对其业务活动进行控制。以三包申请业务为例，企业群A编排了该业务流程为申请→供应商审批→业务员审批→经理审批，若不具有定制权限的用户登录将该流程修改为申请→供应商审批→业务员审批，则会更改整个业务的执行流程，对企业群A造成重大的影响。因此，业务流程编排过程中的安全需求主要是确保具有定制权限的用户对其企业群的业务进行流程编排。

（2）业务流程模型访问过程中的安全需求：产业链协同SaaS平台面向的是不同的企业群，对于各企业群编排的不同的业务流程模型，若企业群A读取并执行企业群B的业务流程，不仅会造成企业群A的业务混乱，而且会泄露企业群B的业务流程。因此，业务流程模型访问过程中的安全需求是确保不同企业群只能访问本企业群定制的业务流程模型。

（3）业务流程模型执行过程中的安全需求：各企业群的业务流程一般包含一个以上的业务活动，而每个业务活动均需要相应的用户来执行。若企业群A的某业务活动被与该业务无关的人执行，则直接影响该业务单据的执行结果。以外出服务申请为例，企业群A编排的流程为申请→制造厂回访→业务员审批→经理审批。在业务员审批活动中，具有执行权限的是相关业务员，若其他人（非相关业务员）进行了审批，则直接影响审批结果，严重影响业务的执行。因此，业务流程模型执行过程中的安全需求主要是保证与该业务单据相关的业务员进行相应的业务活动。

2 基于数字签名及业务实例关联的业务流程安全控制模型

为实现SaaS平台上流程定制及业务流程执行过程中安全性的控制，根据上述分析的安全需求建立如图2的SaaS平台业务流程安全控制模型。为了便于对模型的描述，我们对其涉及的对象进行定义。

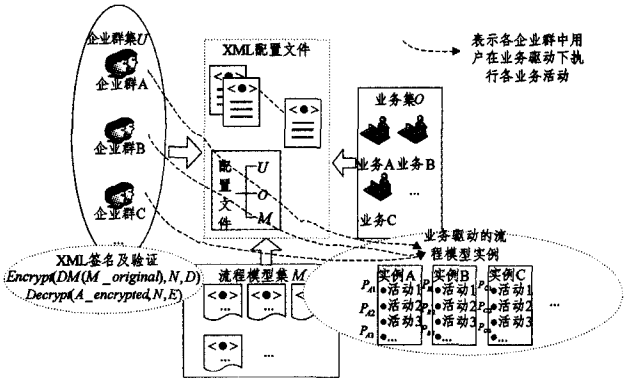


图2 业务流程安全控制模型

定义1 每个业务流程都由一系列的相关活动及一定的顺序组成，其中，每个活动可以由一个五元组 $A_i=(A_{iID},A_{iN},P_{A_i},S_{A_i},C_{A_i})$ 表示，其中：

- A_{iID} 表示活动标识；
- A_{iN} 表示活动名称；
- P_{A_i} 表示具有执行活动的权限标识；
- S_{A_i} 表示活动绑定的状态；
- C_{A_i} 表示活动的性质，如参考、执行、开始等。

定义2 一个业务流程实例可用一个六元组 $FE=(FE_{ID},M_{iID},C_{FE},S_{FE},A_i,T_{FE})$ 表示，其中：

- FE_{ID} 表示流程实例的标识；
- M_{iID} 表示流程模型标识；
- C_{FE} 表示创建该实例的人的标识；
- S_{FE} 表示流程实例的状态，如Running、End、Waiting等；
- A_i 表示流程实例当前运行到的活动；
- T_{FE} 表示实例创建时间。

用户在平台上编排业务流程模型后，为保证编排者的身份，需要进行数字签名，签名的模式可以用如下的形式化描述。

(1)XML 签名模式数学描述

定义 3 XML 签名模式用一个四元组 $Sig=(M\_original_i, DM, UserInf, O_i)$ 表示，其中：

- $M\_original_i \in R(M)$ 表示用户编排的流程模型；
- DM 表示计算摘要所用的算法；
- $UserInf$ 表示编排者信息，且 $UserInf=(User_{Id}, U_i, PriK)$，其中：$User_{Id}$ 表示用户在平台上的标识，U_i 表示用户所属联盟，$PriK=(N,D)$ 表示私钥信息，其中 N 和 D 表示加密参数；
- O_i 表示流程模型所属业务。

定义 4 用 $Abstract_i$ 表示流程模型通过约定的算法 DM 计算得到的摘要，$A\_encrypted_i$ 表示 $Abstract$ 通过加密算法 $Encrypt$ 进行私钥加密后的内容。

由定义 2，可以得到

$$Abstract_i=DM(M\_original_i) \tag{1}$$

$$A\_encrypted_i=Encrypt(Abstract_i, N, D) \tag{2}$$

综合以上两个公式，可得到 XML 签名的计算公式：

$$A\_encrypted_i=Encrypt(DM(M\_original_i), N, D) \tag{3}$$

定义 5 XML 签名验证模式用一个四元组 $CheS=(M\_original_i, DM, UserInf, O_i)$ 表示，其中：

- $M\_original_i \in R(M)$ 表示用户编排的流程模型；
- DM 表示计算摘要所用的算法，由企业群与平台供应商约定；
- $UserInf$ 表示编排者信息，且 $UserInf=(User_{Id}, U_i, PubK)$，其中：$User_{Id}$ 表示用户在平台上的标识，U_i 表示用户所属联盟，$PubK=(N,E)$ 表示公钥信息，N 和 E 表示解密参数；
- O_i 表示流程模型所属业务。

定义 6 用 $V\_Abstract$ 表示系统进行签名验证时采用与加密时相同的 DM 算法对 $M\_original_i$ 进行计算得到的摘要，$D\_Abstract$ 表示 $A\_encrypted_i$ 通过解密算法 $Decrypt$ 进行公钥解密后得到的摘要。

由定义 2，可以得到

$$V\_Abstract=MD(M\_original) \tag{4}$$

$$D\_Abstract=Decrypt(A\_encrypted, N, E) \tag{5}$$

由式(3)—式(5)，可得到签名验证过程为：

$(Decrypt(A\_encrypted, N, E)==MD(M\_original))=$ ture，流程模型真实可靠，可进行存储或升级；

$(Decrypt(A\_encrypted, N, E)==MD(M\_original))=$ false，流程模型被篡改或不为该企业群中有权限的人编排，不进行存储并进行提示。

用户进行数字签名后，系统对其进行签名验证并对相应的业务流程进行存储或升级。基于 SaaS 平台面向多企业群的特点，为确保联盟中的企业在业务的驱动下按照业务与流程的对应关系加载和驱动流程实例，需采用合理的模型存储策略。

(2)流程模型存储策略的数学描述

流程模型存储策略用一个三元组 $Conf=(U,O,M)$ 表示，其中：

$U=\{U_1, U_2, \cdots, U_l\}$ 表示平台上的企业群，l 为平台上企业群数量；

$O=\{O_1, O_2, \cdots, O_m\}$ 表示业务集，m 为业务数量；

$M=\{M_1, M_2, \cdots, M_n\}$ 表示流程模型集，n 表示模型数量。

流程模型存储关系数学描述如下：

① $\forall U_i \in U, \exists R_{ix}(O) \subseteq O$，使 U 和 O 对应关系 $Con(U_i, R_{ix}(O)) \neq \phi$，即平台上任一企业群拥有一个或多个业务，$x$ 为 U_i 对应的 O 的数量。

② $\forall O_i \in O, \exists R_{Oiy}(M) \subseteq M$，使 O 和 M 的对应关系 $Con(O_i, R_{Oiy}(M)) \neq \phi$，即每个业务对应一个或多个版本的流程模型，$y$ 为 O_i 对应的 M 的数量，且 $\forall O_j \in O, O_j$ 对应的版本集为 $R_{Ojz}(M)$，若 $O_j \neq O_i$，则 $R_{Oiy}(M) \cap R_{Ojz}(M)=\phi$，即每个流程模型只能对应一个业务。

$\forall U_i \in U$，设其在平台上编排的流程模型集为 $R_{Uil}(M)$，且 $R_{Uil}(M) \subseteq M$，l 为 U_i 在平台上编排的所有流程模型数。则平台上企业群 U_i 执行其业务 $O_i(O_i \in R_{ix}(O))$ 时，访问其编排的流程模型的路径为：$R_{ie}(M)=R_{Oiy}(M) \cap R_{Uil}(M)$，$e$ 为访问到的模型数，找到 $R_{ie}(M)$ 后，根据版本标记和版本号检测并执行其最新版本 $M_i(M_i \in R_{ie}(M))$，如图 3 所示。

企业群 U \ 业务集 O	O_1	O_2	O_3	……
U_A	$R(M_{A1})$	$R(M_{A2})$	$R(M_{A3})$	……
U_B	$R(M_{B1})$	$R(M_{B2})$	$R(M_{B3})$	……
U_C	$R(M_{C1})$	$R(M_{C2})$	$R(M_{C3})$	……
……	……	……	……	……

图 3 流程定制存储关系

在业务流程执行过程中，为确保与业务相关的对象才能访问业务和执行业务节点，采用基于业务实例关联的模型执行策略。

(3)基于业务实例关联的模型执行策略的数学描述

基于业务实例关联的模型执行策略所涉及的对象由一个二元组 $FB=(FE_i, UserInf_j)$ 表示，其中：

- FE_i 表示某业务实例(如定义 2)；
- $UserInf_j$ 表示执行业务活动的用户的信息，且 $UserInf_j=(U_j, Area_j, Pur_j)$，其中，$U_j$ 表示用户所属企业群，$Area_j$ 表示用户所属片区，Pur_j 表示用户的权限角色。

对于任意业务实例 FE_i，其业务执行策略如下：

$(U_j==U_i(C_{FE_i}(FE_i)) \&\& Area_j==Area_i(C_{FE_i}(FE_i)))=$ true，且 $(Pur_j==P_{A_k}(A_k(M_{ID}(FE_i))))=$ true，则用户 $UserInf_j$ 可以执行当前业务活动 A_k。

3 业务流程安全控制实现的关键技术

3.1 基于 XML 数字签名的业务流程安全编排

数字签名可以保证文件信息的完整性和不可抵赖性，针对编排安全中主要涉及的问题和对象，采用数字签名确认编排的人的身份和流程模型的有效性，以保证平台上的编排安全。XML 数字签名及验证过程如图 4 所示。平台上编排安

全不仅要考虑签名和验证方法，更重要的是如何用该方法解决在平台流程编排过程中的编排安全问题。具体算法如下。

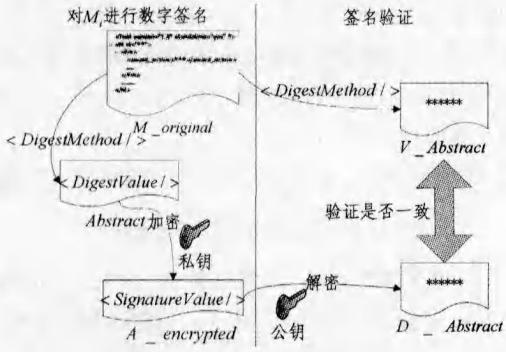


图 4　数字签名和验证过程

算法名称：数字签名解决编排安全算法

输入：业务 O_i，流程模型数据文件 M_original，编排者信息 C_{FC}，签名者私钥 Pri_Key

输出：具有完整性和不可抵赖性的编排结果

BEGIN

Step1　编排者 P 编排 M_i 后，对 M_original 进行保存；

Step2　流程定制机制 WCus_m 执行 Hash(M_original)→Abstract，计算出摘要；

Step3　P 使用优盾及密码提供私钥 Pri_Key，WCus_m 执行 Encrypt(Abstract，Pri_Key)→A_encrypted，并向流程控制机制 WCon_m 发出 Signal；

Step4　WCon_m 执行 Hash(M_original)→V_Abstract；

Step5　WCon_m 根据 C_{FC} 和 Pri_Key，获得 Pub_Key；

Step6　WCon_m 执行 Decrypt(A_encrypted，Pub_Key)→D_Abstract；

Step7　验证 V_Abstract 和 D_Abstract 是否一致：若一致，转至 Step8，否则提示并退出；

Step8　生成 M_i 的版本号 E_N，添加到流程模型信息中，并更新相应 O_i 的版本信息。

3.2　基于业务实例关联的业务流程安全加载与执行

基于业务实例关联的安全执行控制路径如图 5 所示。一个用户 $User_j$ 想要执行业务实例 FE_i 中的活动 A_k，保证执行安全的路径如下：

(1)通过路径 $V(FC,CU)$ 和路径 $V(UU)$，保证业务实例与用户属于同一企业群：首先根据业务实例 FE_i 通过 FC 路径找到创建实例者 C_{FE_i}，再根据 C_{FE_i} 找到其所属的联盟 U，同时，根据 $User_j$ 的信息，找到其所属联盟，判断是否为 U。

(2)通过路径 $V(FC,CA)$ 和路径 $V(UA)$，保证业务实例与用户属于同一业务区域：首先根据业务实例 FE_i 通过 FC 路径找到创建实例者 C_{FE_i}，再根据 C_{FE_i} 找到其所属的区域 $Area$，同时，根据 $User_j$ 的信息，找到其所属联盟，判断是否为 $Area$。

(3)通过路径 $V(FM,MA,AP)$ 和路径 $V(UPu)$，保证用户具有执行 A_k 的权限：首先根据业务实例 FE_i 通过 FM 找到其所属业务流程模型 M_{ilD}，再根据流程模型通过 MA 找到相应的活动 A_k，通过 A_k 找到相应的权限 P，并判断 $User_j$ 是否具有权限 P。

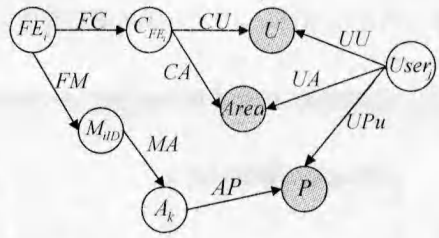


图 5　基于业务实例关联的安全执行控制路径

对于以上用户执行业务实例中活动的 3 条路径，其判断及执行的规则如下：

①3 条判断路径的优先级为：$Pri(U)>Pri(Area)>Pri(P)$；

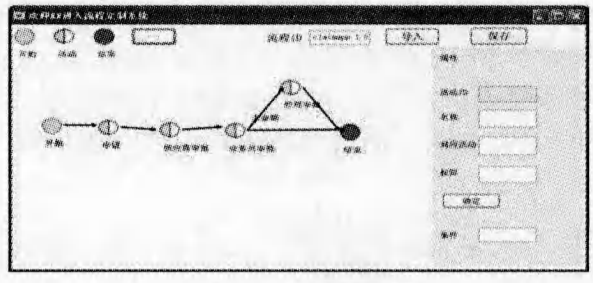
②如果高优先级的路径不被满足，则直接不进行其他优先级的路径的判断。

③当 3 条路径同时满足时，用户 $User_j$ 才能执行 A_k。

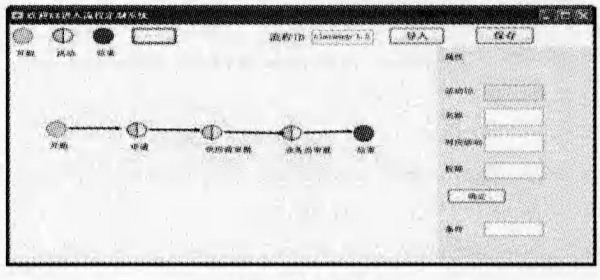
4　业务流程定制中的安全验证

4.1　某企业群三包申请业务流程修改验证

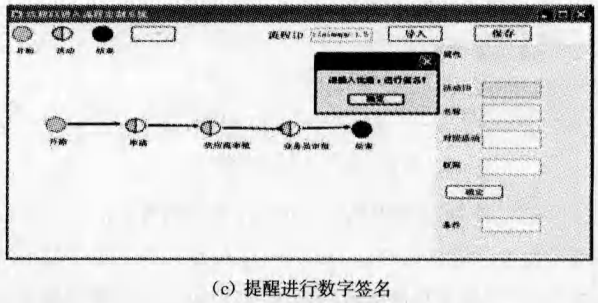
(1)假设某人盗用企业群 A 的龙头企业中具有编排权限的用户的账号来登录并导出之前编排的三包申请业务流程，如图 6(a)所示。修改后如图 6(b)所示。点击保存后，弹出提醒插入优盾并进行数字签名，如图 6(c)所示。如果不插入优盾，则不能对编排的流程进行升级。



(a) 导入的三包申请业务流程



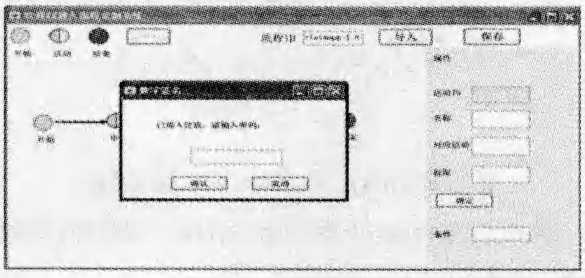
(b) 修改后的业务流程



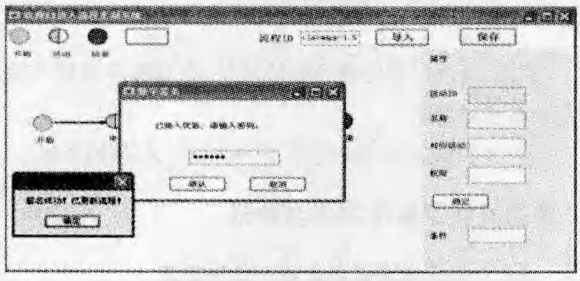
(c) 提醒进行数字签名

图 6　某企业群三包申请业务流程修改验证

(2)企业群 A 的龙头企业中具有编排权限的用户进行上述修改,插入优盾后,如图 7(a)所示;输入密码确认后,如图 7(b)所示。



(a) 插入优盾后输入密码



(b) 签名成功并更新流程

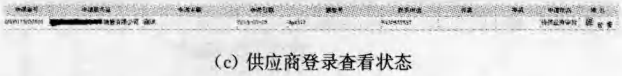
图 7 企业群龙头企业业务流程修改验证

由以上实验可以看出,平台上的业务流程的编排只能由龙头企业中通过签名认证的人修改,其它人无法修改。

(3)以上实验中企业群 A 对本企业群的三包申请业务流程进行升级后,创建一个三包申请业务单据,单据号为 0500113032801,如图 8(a)所示。企业群 A 中的业务员登录查看其状态如图 8(b)所示,但无法对其进行管理(审批)。企业群中的供应商登录进行查看,可对其进行管理,如图 8(c)所示。

(a) 创建单据

(b) 业务员登录查看状态



(c) 供应商登录查看状态

(d) 供应商审批通过后查看状态

图 8 业务流程编排方法的有效性的验证

由以上实验可以看出,企业群 A 在修改自己的三包申请业务流程后,其业务流程执行正确,可以验证业务流程编排方法的有效性。

4.2 不同企业群三包申请业务流程加载和执行验证

企业群 B 编排的三包申请业务流程为申请→制造厂回访→业务员审批,创建一个业务单据,单据号为 0600513032801,企业群 B 的制造厂登录,只能查看本企业群单据,不能查看企业群 A 的单据(0500113032801),且单据状态如图 9 所示。

图 9 企业群 B 中的制造厂查看状态

由 4.1 节的实验和本实验可以看出,同样是三包申请,企业群 A 和企业群 B 均执行的是本企业群定制的业务流程,说明不同企业群对于相同业务调用和加载不同的业务流程,不同的单据关联不同的企业,只有与此单据相关的企业才能访问,不相关的企业无法访问。

结束语 流程定制已逐渐成为产业链协同 SaaS 平台上不可缺少的功能,各企业群定制的业务流程对其业务的控制过程起着关键的作用,一旦其安全性不能保证,则会对企业业务造成重大影响。本文根据流程编排及控制过程周期分析其存在的安全需求,建立了基于数字签名及业务实例关联的业务流程安全控制模型,并提出了其实现安全控制的关键技术。上述两个实验结果可以验证该安全技术的有效性。

参 考 文 献

[1] 周亮,曹健,陈姣娟. 软件即服务流程模型的自动演化[J]. 计算机集成制造系统,2011,17(8):1603-1608

[2] Thomas K, Thao N, Linh L. A software as a service with multi-tenancy support for an electronic contract management application[C]// 2008 IEEE International Conference on Services Computing. Hawaii, 2008: 179-186

[3] Zhang Kuo, Zhang Xin, Sun Wei, et al. A policy-driven approach for software-as-services customization[C]// Proceedings of the 9th IEEE International Conference on E-Commerce Technology (CEC) and the 4th IEEE International Conference on Enterprise Computing(EEE). Tokyo, Japan, 2007: 123-130

[4] Li Ya, Wang Hai-rui, Zhang Zhibin. Multi-Agent Based Workflow Management Systems Design[M]. Adv. Scl. Lett. 6, 2012: 727-731

[5] 曹健,李明禄,张申生. 基于多 Agent 协商的服务流程定制[J]. 计算机学报,2006,29(7):1116-1124

[6] 史玉良,栾帅,李庆忠,等. 基于 TLA 的 SaaS 业务流程定制及验证机制研究[J]. 计算机学报,2010,33(11):2055-2066

[7] 高嵩,欧阳昱,刘玉树. 工作流模型的有向图表示及基于 Petri 网的验证方法[J]. 计算机仿真,2004,21(6):182-184

[8] Stormer H, Knorr K. A model for security in agent-based workflows[J]. INFORMATIK/INFORMATI- QUE, (6): 24-29

[9] 琚洁慧,吴吉义,章剑林,等. SaaS 应用中的多租户与安全技术研究[J]. 电信科学,2010,10:41-46

[10] 王菽兰,李晓桓,李伟. 基于 SaaS 的物流信息系统安全性机制研究[J]. 信息安全与技术,2012:36-38

[11] 王凯,张毅坤,杨凯峰,等. 面向 OA 系统的工作流引擎研发[J]. 计算机工程与设计,2008:4967-4970