基于SPKI电子支付中的银行端访问控制*)

王 茜 王富强 傅鹤岗 朱庆生
(重庆大学计算机学院 重庆400044)

Bank Access Control of Electronic Payment Based on SPKI

WANG Qian WANG Fu-Qiang FU He-Gang ZHU Qing-Sheng
(Computer Department of Chongqing University, Chongqing 400044)

Abstract In the system of electronic payment based on SPKI, access control of bank acts as the important function of identification, protecting customer's privacy and ensuring payment. The paper proposes the model of bank access control, and describes the frame and the steps of the access control. Finally, the paper analyzes the characteristics of the model.

Keywords Electronic payment, SPKI, Access control

1 引言

近年来,随着Internet的普及,基于Internet的电子商务也得到迅速发展。但是安全支付体系、信用体系及配送体系等方面的滞后,严重制约着我国电子商务的快速发展。电子支付是其中关键的制约因素。

目前主要有四类电子支付系统:在线支付卡系统、在线电子现金、电子支票和基于智能卡的电子现金[5]。由于参与的各方通过网络进行交易,电子支付通常需要对参与方进行鉴别。现有的支付协议中大多基于PKI的认证机制,其存在的问题是系统过于复杂,需要建立庞大的基础设施来支持,其结构不符合真实的网络空间的需要,严格的层次结构和中央集权的认证方式,提供的是身份认证来识别实体,个人交易行为容易被他人追踪而泄漏个人隐私和组织的结构。鉴于此,我们提出了一种新的支付协议,本文简要地描述了其流程,并着重就银行端的访问控制进行了阐述。

2 SPKI简介

简单公钥基础设施SPKI(Simple Public Key Infrastructure)是一个为访问控制定义公钥证书的Internet草案标准。

SPKI证书用公钥代替名字,直接将公钥与授权绑定在一起,使得SPKI证书常常可以独立于任何命名机制而自由使用。SPKI证书由资源所有者或服务提供者向使用者颁发,当访问者向服务提供者提出访问请求时,该证书用作访问授权的凭证。SPKI证书为一个由颁发者签名的五元组:〈Issuer, Subject, Delegation, Authorization, Validity Dates〉,其有如下特点[2,4]:(1)用公钥代替名字,权限直接授给公钥,由于公钥具有全球唯一性,回避了名字重复的问题;(2)证书可以由资源所有者或服务提供者根据实际控制的需要自由生成,不需要集中的第三方作为认证权威,更方便有关各方的使用和相关系统的实现,同时也更加经济;(3)访问授权可以被传递,任何获得了可再授权证书的实体都可将自己得到的授权全部或部份转授给其它实体;(4)授权可以根据具体应用的不同自由定义,因此访问控制授权的适用范围基本不受业务限制;(5)对证书规定了明确的有效期。

SPKI机制的主要思想是通过公钥证书对某些行为进行授权,其目标是可以根据管理者的安全策略建立起一个分布式的安全体系。根据SPKI的这一思想和它的特点,结合电子支付的需求,我们建立了一个基于SPKI的支付系统,该系统以支付者(客户)的银行账户作为支付保证,支付行为通过银行签发给客户及客户签发给商家的支付授权SPKI证书来进行授权,这些都建立在银行端对银行账户的访问控制基础之上。因此,银行端的访问控制在整个支付过程中实际上起到了保证支付和类似身份认证的关键作用。这在没有建立起完善的认证和信用体系的情况下,更有特别重要的意义,同时它也简化了支付系统的实现。

3 基于SPKI的电子支付系统

利用SPKI证书的以上特点,我们提出了基于SPKI的电子支付系统模型,在这种模型框架之下,可以支持B2C交易的匿名电子支付的实现。模型的整体框架如图1所示。

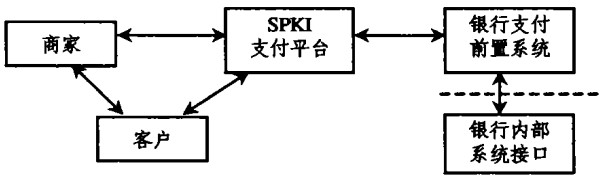

图1 基于SPKI的电子支付系统模型

基于上述模型的交易过程如下:

(1)初始阶段

1)客户到银行开设账户(如果有现存账户则可用之);

2)客户向银行提交公钥,向银行申请SPKI证书;

*)基金项目:重庆市科技攻关项目(7220-13-15)。王 茜 副教授,主要研究方向:电子商务、远程教育。王富强 硕士生,研究方向:电子商务、网络安全。傅鹤岗 副教授,主要研究方向:软件工程理论及应用、软件工具及环境。朱庆生 教授,主要研究方向:电子商务、多媒体数据压缩、网络信息系统及软件开发环境。

3)银行向客户颁发 SPKI 证书,同时将证书中的公钥与客户的帐号进行绑定;

4)商家和银行到 SPKI 支付平台注册,并申请 SPKI 证书。

(2)购买阶段

1) 客户获取商家的商品信息(可以从网上浏览,也可从其他渠道获得);

2) 客户通过商家网站或商家提供的其他方式,将订单传送给商家;

3) 商家收到客户订单后,将订单所列项目、应付账款、交易标识号和商家的 SPKI 证书一起发给客户;

4) 客户确认后点击支付命令,启动支付程序,客户向商家签发一次性支付授权证书(SPKI 证书)。支付程序向 SPKI 支付平台发送支付指令,包括交易标识号、金额、客户证书(链)、客户签发给商家的一次性支付授权证书。

5) SPKI 支付平台收到支付指令后,通过自己存储的银行公钥对商家进行验证。通过验证后,根据客户开户银行的不同,将支付指示转发到相应的客户帐户银行。如果没有通过验证,则向客户发出反馈信息。

6) 客户银行的前置系统验证证书和请求的合法性,对客户的支付请求进行访问控制,并将请求处理结果反馈给 SPKI 支付平台。

7) 如果支付成功,支付平台将处理结果分别反馈给商家和客户,如果没有成功,则把原因反馈给客户。

该支付模型具有安全、不需要统一的认证中心、可实现匿名支付、交易可追踪、良好的可扩展性、容易构建等特点。

4 银行端的访问控制模型

4.1 访问控制模型实现框架

银行端的访问控制是通过银行支付前置系统来完成的,其模型框架如图2所示。

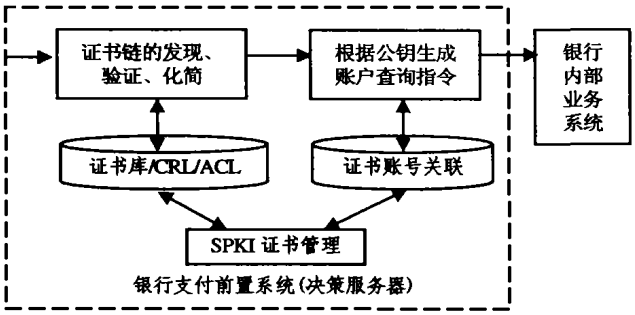

图2 银行端的访问控制模型框架

访问控制的实现步骤为:

(1)客户到银行开设账户,此时银行应按有关政策核查用户资料。

(2)客户向银行提交公钥和账户证明,向银行申请 SPKI 证书。银行在验证了客户提交的相关资料后,为客户颁发 SPKI 证书,该证书由一个五元组组成,issuer 为银行公钥,subject 为客户公钥,delegation 为 True,authorization 为访问授权,如为了控制风险而规定的一次可以最多支付的上限等,另外还要明确指定证书的效期。其结构如图3所示。与此同时,银行还要把证书存入证书库,并在关联库中把客户的公钥和帐户信息绑定在一起。

客户也可以根据需要向其亲友签发类似的 SPKI 证书,此项功能可以由客户端软件来提供并进行相应管理。

(3)在支付时,支付前置系统接收来自 SPKI 支付平台转发而来的客户支付指示和绑定的商家交易信息(如交易编号)以及证书链。通常情况下这个证书链由银行签发给客户的证书以及客户签发给商家的一次性支付证书组成。由于 SPKI 证书机制可以签发证书进行转授权,因此客户证书本身可能也是一个证书链,如客户证书和她签发给其亲友的证书组成的证书链。

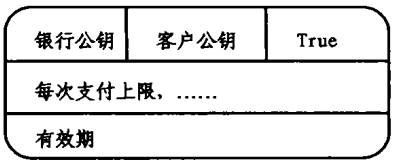

图3 银行颁发给客户的 SPKI 证书结构

(4)支付前置系统收到上述信息后,要对请求和相伴随证书链的一系列数字签名进行验证。然后检查证书链中的证书是否已被撤消,再检验证书链是否完整,即检查能否从 ACL 到客户证书,最后到商家证书形成一条通路。如果证书链完整,对该证书链用简化算法对其进行化简,最后得到一个简化后的五元组。从这个五元组的有效期和得到的授权可以判断出商家是否有权访问客户的账户从而取得支付授权。如果客户提供的证书链不完整,可以拒绝服务或要求客户重新提供完整的证书链,若前置服务器有足够的性能可用,也可以在自己的证书库中为客户搜索缺失的证书。

(5)如果五元组有效性条件得到满足,前置系统将根据客户的公钥在本地的证书账号关联库中找到该客户的账户信息,再把该账户信息与先前得到的五元组访问权限相结合,生成一个符合银行业务系统接口的查询指令,把该指令转入银行内部的业务系统。

(6)业务系统接收到来自前置系统的查询指令后,在生产数据库中访问相应的客户账户资料,如有必要和可能,对账户冻结一定数量的余额,作为支付准备,然后和向前置系统返回一个"成功"的支付应答。如果客户账户余额不足本次支付请求,或其他原因导致账户不能使用,则向前置系统返回相应的错误信息。

(7)前置系统收到业务系统的反馈信息后,转发给 SPKI 支付平台。

4.2 模型的特点

上面的访问控制模型和实现步骤,具有如下特点:

(1)用公钥来代替用户身份或名字,并且将用户的公钥与用户的账户通过银行前置系统的关联库绑定起来,这样就可以有效地防止在银行之外传输账户资料等敏感信息,同时也减少了传输和加密的数据量。由于在银行之外的任何传输都不包含任何账户信息或其他敏感信息,无论对商家、客户,还是对 SPKI 的支付平台来说,可见的与身份有关的信息只有一个公钥证书,所以要想知道其他参与方的账户信息都是不可能的。因此,通过银行端的访问控制,可实现完全的匿名支付,满足了保护客户和商家、隐私的需求。

(2)如果发生交易纠纷或司法需要,根据客户和商家提供的交易记录,结合银行的支付记录和公钥账户关联库,可以追踪整个交易的来龙去脉。但是仅凭某一方的记录,没有银行的参与是做不到的。这样既有效地保护了满足私密性,又满足了司法和解决纠纷的需要。

(3)通过银行向客户颁发SPKI证书,从而对客户账户进行有效的访问控制,以及SPKI支付平台向商家和银行颁发SPKI证书,信任体系不依赖于官方证书认证体系的建设,可以自成体系。

(4)在银行端采用前置系统进行访问控制,可以提高效率,不会对银行内部的生产系统产生太大的负担,同时也可以通过防火墙形成一道安全屏障。

(5)如果客户提交的证书链有缺失,前置决策系统如果性能允许,可以在证书库中代为搜索。

结束语 SPKI作为一种面向公钥的授权机制,可以很好地支持分布式访问控制。将其用于支付系统,可以不依赖于统一的认证中心,具有良好的可扩展性且容易构建。在我们开发的基于SPKI的支付系统中,通过银行端的访问控制,有效地支持了授权支付的完成,可实现网上的匿名支付,如有需要,也可实现交易的追踪。

参考文献

1 Ellison C. SPKI Requirements[S]. RFC2692. Sep. 1999

2 Ellison C, Frantz B, Lampson B, et al. SPKI Certificate Theory [S]. RFC2693. Sep. 1999

3 Heikkila J, Laukka M. SPKI Based Solution to Anonymous Payment and Transaction Authorization [J/OL]. http://www.tml.hut.fi/Research/TeSSA/Papers/Heikkila-Laukka/nordsec99-heikkila-laukka.pdf.

4 Saito T, Umesawa K, Okuno HG. Privacy-enhanced Access Control by SPKI and Application [A]. Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000. (WET ICE 2000) [C/CD]. In: Proc. IEEE 9th Intl. Workshops on, 2000. 201～206

5 Lee Z-Y, Yu H-C, Kuo P-J. An Analysis and Comparison of Different Types of Electronic Payment systems[J/OL]. http://www.cs.tcd.ie/～htewari/4D1/papers/payment.pdf.

(上接第171页)

DBBook: = book [title [String], publisher [String], price [String], year [Int]];

进行集成图书信息查询时,定义的数据类型为:

INTEcatalog1: =books * SEArchbk1;

SEArchbk1: =book[publisher [String], year [Int]];

INTEcatalog2: =books * SEArchbk2;

SEArchbk2: =book[title [String], price [String]];

假如我们通过INTEcatalog1或INTEcatalog2,查询2001年以后出版的图书信息,查询语句用YATL写为:

```
define q($x): = make books [ * book[title[$t], publisher
    [$n]]]
        match $x with
    books [ * book[@year[$y], title [$t], publisher
    [$n]]
where $y>2001
```

上述查询对应的数据类型为:

INTEcatalog: =books * SEArchbk;

SEArchbk: = book[title [String], publisher [String], year [Int]];

因为INTEcatalog1没有定义title而INTEcatalog2没有定义publisher,所以无论从INTEcatalog1或INTEcatalog2都不能得到查询结果,我们用部分包含关系解决这个问题。

设DBCatalog对应的XML模式为S_1',对应的数据库为D,INTEcatalog1和INTEcatalog2对应的XML模式分别为S_1和S_2,查询的关键字为title、publisher、year,对应的模式为S',查询过程如下:

STEP1:由算法2(1)-(5)找出Sq=$\{S_1, S_2\}$;

STEP2:由(6)-(7)找出存在部分包含关系的模式集合S=$\{S_1, S_2\}$及部分包含关系θ_1;

STEP3:(9)调用算法1求最大下限(LUB)对模式重组,得到模式S_0;

STEP4:(10)由S_0与S'的关系θ_1,S_0与S_1'的关系θ_2,S_1'与D的关系θ_3,通过计算关系$\theta_1 \infty \theta_2 \infty \theta_3$,得到查询结果。

讨论 本文对XML数据类型模式之间提出了部分包含关系的概念,并就存在部分包含关系的XML模式,利用部分包含中的多对一关系,使用求最大下限的方法,组合出所需的数据类型模式,以完成有效的查询。在实际查询中,定义出所有的数据类型也是不现实的,可以在定义出主要的数据类型后,对需要查询的次要元素的数据类型定义为Any型,在必要时对Any数据类型进行扩展,以得到需要的查询结果;另外,在实际问题中,不同关系实体之间的多对多关系也经常出现,对于XML数据类型之间的多对多关系本文未进行研究。

参考文献

1 Kuper G M, Siméon J. Subsumption for XML types. ICDT 2001 LNCS 1973, 2001. 331～345

2 Clmet S, Siméon J. YATL: a functional and declarative language for XML. Draft manscript Mar. 2000. http://www-db.research.bell-labs.com/user/simeon/icfp.ps

3 Fernandez M F, Siméon J, Wadlor P. XML query languages: Experiences and exemplars. draft manuscript, communication to the W3C, Sept. 1999

4 Mercer D. XML编程起步. 北京:人民邮电出版社,2001

5 Deutsch P B A, Fan W. Beyond Xml Query Languages. November 18, 1998. http://www.w3.org/Tands/QL/QL98/pp/penn.ps

6 张国钢,王建华,武安波,耿英三. 基于XML的电气图描述语言的设计与实现. 计算机工程与应用,2002,38(18):47～49

7 Mertz D. XML and Data Models: Hierarchical, Relational and object-oriented. March 2001 http://gnosis.cx/publish/programming/xml_masters_8.txt