一种基于SPKI的匿名支付方案*)

朱庆生　李唯唯　王　茜　傅鹤岗
（重庆大学计算机学院　重庆400044）

An Anonymous Payment Scheme Based on SPKI

ZHU Qing-Sheng　LI Wei-Wei　WANG Qian　FU He-Gang
(Computer College, Chongqing University, Chongqing 400044)

Abstract SPKI is a proposed standard for public-key certificates. One important property of SPKI is that SPKI is key-oriented rather than name-oriented, and the public-key is globally unique. In this paper we propose an anonymous paymentscheme based on SPKI aiming at the problem of anonymous payment in B2C e-commerce. In the scheme we use the key-oriented characteristic of SPKI to link the public key to the account, and use authorization certificates to pay. The scheme achieves the anonymity very well.

Keywords SPKI, Anonymous payment, Authorization certificates, E-commerce

1. 引言

随着世界进入知识经济时代，信息化、网络化成为社会经济发展的潮流和趋势，基于Internet的电子商务在世界范围内已成为发展最快的产业之一。对应于此，在Internet上许多安全技术也迅速发展，以保障客户在电子商务交易中的安全。特别是目前B2C电子商务模式的发展，支付中的匿名性已逐渐成为一个热门的话题。由于种种原因，客户在商业交易中常常希望保护自己的隐私，不愿泄露自己的身份、购物习惯、购物品种和数量等信息。在现金交易中一般可以很有效地保护客户的身份，钞票虽然有号码，但通常不会暴露使用者是谁。但在电子交易中，由于支付协议的需要通常会记录用户的许多私有信息，这不利于客户。我们知道，匿名性并不是一个新的话题，它的主要目标是使我们的电子交易具有更完美的安全性[4]。因此，在电子商务中，用户的匿名性是安全性考虑的一个重要方面。如电子现金的匿名性[5]以及第三方代理等都是从这方面考虑的。

2. 方案的提出

通常解决电子商务支付匿名性的方案有电子现金或采用第三方代理。

电子现金是目前较为普遍的实现匿名支付的方案。电子现金是以电子化数字形式存在的现金货币。电子现金的发行方式包括存储性质的预付卡（即电子钱包）和纯电子系统形式的用户号码数据文件等形式。电子钱包也可以看成是电子现金的一种形式，往往和智能卡结合使用。利用电子现金可以实现支付中的匿名性。客户只需预先在银行获取电子现金，然后就象使用实际现金一样购物。购物过程中不可能接触到用户的个人信息。在电子现金交易中，消费者先到开展电子现金业务的银行开设帐户并在帐户内存钱，然后从银行提取和在自己的计算机上存贮电子现金。制造电子现金的银行验证现有电子现金的有效性和把真实的货币与电子现金交换。商家能够在提供信息或货物时接受支付的电子现金货币。在整个过程中，支付者的身份是不公开的。使用电子现金要求银行和卖方要有协议和授权关系，银行负责买方和卖方之间资金的转移。虽然电子现金可象实际现金一样具有灵活性，可以存、取、转让，而且安全性也比较好，但它也有自己的缺点。它仅适合于小量的交易，而且就和普通的货币一样，硬盘故障的时候，如果没有备份，现金就丢失了。

第三方代理方案是指买方和卖方通过共同信任的第三方来完成交易的支付过程。这种方式的特点是：支付是通过双方都信任的第三方完成的；信用卡信息不在开放的网络上多次传送，买方有可能离线在第三方开设帐号，这样买方没有信用卡信息被盗的风险；卖方信任第三方，因此卖方也没有风险；买卖双方预先获得第三方的某种协议，即买方在第三方处开设帐号，卖方成为第三方的特约商户。通过这种方式使卖方看不到买方的信用卡等信息，对卖方来说买方是匿名的。而且这样也避免这些信息在网上多次公开传输而导致信息被窃。这种方式也有其缺点，首先是客户和商家双方都需在第三方上注册，这个第三方必须是客户和商家都严重信任的第三方。如果第三方出现假冒，系统毫无安全性可言。其次，在支付过程中还是与信用卡号等关键信息相关联，存在潜在的安全隐患。

SPKI(Simple Public Key Infrastructure)是IETF提出的一个公钥证书标准[1]。它主要用于访问控制。访问控制就是对受保护的资源的访问进行控制，它主要的目的就是确信只有授权用户可以访问受保护的资源。访问控制系统是基于访问控制列表ACL(Access Control List)。访问控制列表就是一系列形成证书链的条目列表。每一个资源都与一个授权用户列表相绑定。访问控制列表是证书授权的来源。SPKI强调分布式并且在应用中使用公钥而不是名字。SPKI证书是基于公钥加密。不论是产生SPKI证书或使用SPKI证书，私钥和公钥都起着主要的作用。除了用于访问控制之外，SPKI还可用于名字证书。SPKI证书需要满足的基本要求是：1. 证书可以自由产生。也就是说，每个人都可以自由地签发证书并授权给其他用户。这不需要中心的授权机构和注册的实体。2. 权力可传递。即一个人可以将他的权力转授给其他人。3. 授权可以自由定义和分发。4. 证书必须清楚地注明有效期[2]。SPKI还有一个重要的特点是它不是面向名字而是面向公钥，公钥的一个非常重要的特点就是全球唯一。一个公钥可能很长，因此公钥可以用来标志一个对象。相对于公钥来说，名字就有其局限性，它通常不能够全球唯一。通常，名字只用来在局部范围内标志一个对象。由于SPKI强调公钥而不是名字，我们可以将

*)重庆市科技攻关项目(编号2002-7220)资助。朱庆生　教授，研究方向为多媒体技术、电子商务、计算机网络。李唯唯　硕士生，研究方向为电子商务。

权力直接赋给公钥。这样，SPKI 就可以避免将公钥和名字绑定的问题。

由于 SPKI 的这些特点，在本文中，我们提出一种基于 SPKI 的匿名支付方案，这个方案不仅能有效解决匿名支付的问题，而且克服了本节前面提到的电子现金和第三方代理方案的不足之处。该方案应用在重庆市科技攻关项目——基于 SPKI 的安全多渠道电子商务支付系统中。

3. 基于 SPKI 的匿名支付方案

3.1 授权证书结构

基于 SPKI 的安全多渠道电子商务支付系统主要的功能模块有支付平台、银行端、客户端和商家四部分组成。在整个支付过程中，各方相互之间的认证以及授权的发生都是通过授权证书来实现的。本方案所设计的授权证书结构遵循了 SPKI 证书结构的标准，其结构如图1所示。

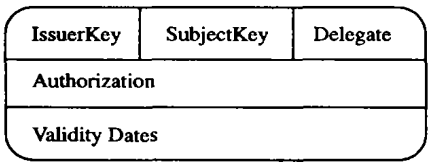

图1 授权证书结构

IssuerKey 域是证书签发者的公钥，表明了是谁签发出或签发了证书。签发者的公钥有一个对应的私钥，它用来签发证书。SubjectKey 域也是一个公钥，它是被授予权力者的公钥，表明了是谁接受证书授予的权力。Delegation 域是一个布尔值，如果值为“真”，表明被该证书授予权力者可以将证书授予的权力进行再授权，也就是权力的传递。如果值为“假”，则不能进行再授权。Authorization 域是证书签发者定义的可供访问的权力。Validity Dates 域有一个不早于的时间和不迟于的时间，用来表明一个证书的有效期。

以上描述的授权证书结构的内容在经过证书签发者的私钥签名后就是授权证书。可以看到，这种证书设计无论是银行签发给客户的证书或客户签发的再授权证书，都只有证书签发者和证书接受者的公钥，而不会暴露客户的相关个人信息，保证了客户在支付过程中的匿名性。

3.2 匿名支付流程

本方案匿名支付流程如图2所示。

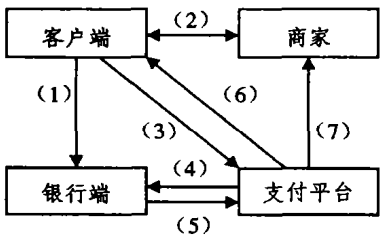

图2 匿名支付流程图

从图2的匿名支付流程图中可以看到，这个匿名支付方案的实现分为以下几个步骤。

第1步：客户信息的注册。客户首先需要在银行开设一个帐户，这是支付的前提。其次，客户需要产生一对密钥在授权中将会用到。值得注意的是，产生这对密钥的途径可以是客户自己产生或者是由银行代替客户产生，但必须要保证这对密钥的安全性，不能泄露这对密钥，否则就有可能有人假冒该用户。然后，用户为了实现支付，需要获得证书。用户与银行联系，银行要验证用户的身份并验证其是否有权使用相关帐号。在实际中，我们并不需要对于银行的匿名性，因此银行有客户的相关资料。在获得证实后，客户就告诉银行需要关联到证书的帐号，银行就将用户提供的公钥和帐号联系起来[3]。如果证书中的授权得到接受，银行就用自己的私钥对证书进行签名，而银行的公钥已广泛地公开，因为银行并不需要保持匿名。银行签发的证书如上一小节所述，包含了银行的公钥(IssuerKey)，即证书的签发者，客户的公钥(SubjectKey)，即证书授予权力的接受者，银行是否允许客户将权力进行进一步授权的标志(Delegate)，银行授予客户的具体权力(Authorization)，以及证书的有效期(Validity Dates)。在这里我们可以看到，用户的帐号并不出现在证书中，因为如果有了帐号就破坏了匿名性。证书的签名也是非常重要的，它证明这的确是银行签发的证书，而不是一些假冒者。现在，客户获得了证书可以进行支付了。

第2步：客户与商家进行信息交换。在这个过程中客户首先选定购物的具体内容，然后在向商家进行购物内容确认时将自己的公钥送往商家。商家将向客户返回商家的公钥、购物清单和帐号，这个帐号就是客户将要转帐的帐号，并用客户的公钥对这些信息进行加密，以防止在信息传送过程中被窃取。

第3步：客户的支付行为。当客户需要支付时，客户就签发一个有相关支付信息的 SPKI 授权证书，并将这个证书和完整的证书链送到支付平台。这个与支付相关的授权证书实际上也是客户将银行授予他的私有证书进行的再授权，其证书结构也如3.1节所述，有客户的公钥(IssuerKey)和商家的公钥(SubjectKey)，以及再授权标志(Delegate)，授予的权力(Authorization)和证书的有效期(Validity Dates)。在客户签发支付信息的这个过程中也没有客户的帐号和相关信息的传递。在这里，我们要求客户提供完整的证书链，如果证书链不完整，需要客户进行补齐。证书链可以存放在客户所使用的终端里。

第4步：支付平台将客户的支付信息送往银行。支付平台在接收到客户的证书中，并没有帐号和客户的相关信息，因此对于支付平台来说，客户是匿名的。当客户向支付平台提出支付请求后，支付平台做出响应，搜索客户开户银行相对应的区域(因为本系统在设计整体时考虑了一个比较大的范围，因此存在许多区域，每个区域有其对应的支付平台)，验证商家的身份，在商家身份获得确认后将客户的支付请求用支付平台的私钥进行签名，签发一个 SPKI 授权证书。如果支付请求与客户所在开户银行在同一个区域，则支付平台直接将该授权证书送往银行。如果支付请求与客户所在开户银行不在同一个区域，则根据前面搜索的结果将授权证书送往相应区域的支付平台，进行签名后再送往相应银行。这里平台之间签发证书进行信息的传递也应加入客户的证书链，以便为银行验证证书链的完整性提供依据。支付平台的签名主要是为了防止假冒，并且支付平台在此可屏蔽掉客户的购物清单，这样银行看不到客户的购物内容，保护了客户的隐私性。

第5步：银行验证支付平台和客户的证书，以及客户提供的证书链的完整性，并响应支付请求。银行在接收到支付平台送来的客户支付请求后，首先利用支付平台的公钥验证支付平台的签名。在证实支付平台的身份后，对客户提供的证书链验证其完整性。如果证书链的完整性得到证实，就对证书链进行约简，并利用客户的公钥验证客户的签名。若所有条件符合，就进行实际支付行为，即转帐，并向支付平台返回成功信息。如果其中有一个条件不符合，银行就会拒绝支付平台的支付请求，并向支付平台返回不成功的信息。

第6步：支付平台向客户返回银行反馈的成功与否的信息以便客户能及时了解到交易的情况。

第7步：支付平台向商家返回银行反馈的成功与否的信息，让商家知道交易是否成功，以便商家做好相应的准备，如是否准备发货等。

4. 性能分析

本文所设计的电子商务支付，是一个基于 SPKI 的匿名支付方案。下面我们对这个方案进行评价。

匿名性：该方案是将客户的帐号和公钥进行绑定。在整个支付过程中，只有银行知道客户的具体身份和帐号，对于商家和支付平台而言，客户都是匿名的。对于银行来说，客户没有必要匿名，因此这个方案很好地实现了匿名支付。

不可伪造性：SPKI 的证书在签发和传递中都有证书签发者的私钥进行签名，这样可防止一些假冒者进行伪造。

交易的可追踪性：虽然在通常的支付中，客户都是匿名的，但在特殊情况下（如系统的安全性受到攻击），根据需要我们是可以在银行端查到客户的支付信息，从而可以查到资金的流向。

支付的灵活性：由于我们是将客户的公钥和帐户绑定，只要帐户里有足够的金额，并且在银行得到相应金额的授权证书，则客户可以在电子商务中进行小面额、大面额等多种形式的交易，这可以用 SPKI 证书中的 Authorization 域加以限制条件，以实现对支付额度的控制。而且 SPKI 证书支持再授权，SPKI 的这种可再授权的特点还使得这种支付方式可以象电子现金支付方式一样灵活地进行转让、存、取等操作。

安全性：由于证书中只有客户的公钥，即使证书在传递或保存过程中被窃取或丢失，也不会造成经济上的损失。它不象电子现金一样，没有备份或丢失了以及硬盘故障的时候就没有了。而且得到该公钥的人也获取不到与该公钥相对应的客户的相关信息，不象第三方代理在支付过程中还是与信用卡号等关键信息相关联，存在潜在的安全隐患。客户只需要再产生密钥对到银行去重新关联帐号即可。这有效地保障了客户资金的安全。

结束语 在本文中，我们针对 B2C 电子商务的发展中，客户对电子商务中支付的匿名性要求日益提高的问题，提出了一个适用于 B2C 电子商务支付的基于 SPKI 的匿名支付方案。由于 SPKI 强调使用公钥而不是使用名字，因此该支付方案中，客户只公布自己的公钥，而不会泄露其他私人信息，很好地实现了支付的匿名性和保护了客户的隐私。而且，虽然支付匿名，但在客户注册的银行端有客户的详细信息，在必要情况下也可对客户的行为进行追踪。因此本方案在实际中有其实用性。

参 考 文 献

1 Ellison C, Frantz B, Lampson B, Rivest R, Thomas B, Ylonen T. SPKI Certificate Theory, SPKI Reuirements. RFC 2693. Sep. 1999

2 Ellison C. SPKI Requirements. RFC 2692. Sep. 1999

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

4 Kesdogan D. Evaluation of Anonymity Providing Techniques Using Queuing Theory. In: The 26th Annual IEEE Conf. on Local Computer Networks, Paper Session #4, 2001

5 Claessens J, Preneel B, Vandewalle J. Anonymity Controlled Electronic Payment Systems[A]. In: Proc. of the 20th symposium on information theory in the benclux [c], Belgium: Haasrode, 1999. 109～116

（上接第151页）

在包延迟时最大可容忍延迟变化。

用 t_{inter} 表示同一个包中两个 RLC 块之间的时间，T_{inter} 表示相邻两个包之间的间隔时间（即第 i 个包中的最后一个 RLC 块和第 i+1个包中第一个 RLC 块时间），如图7所示。

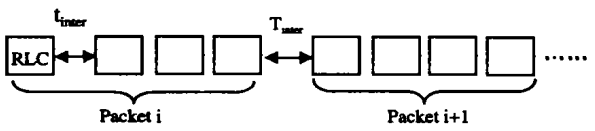

图7 RLC 块之间与包的关系

假设第 i 个包的延迟时间为 D_i，由于：$D_i = T_{inter} + \Sigma t_{inter}$，为了能够满足数据流的实时性需要，调度模块必须要保证：$T_{inter} + \Sigma t_{inter} \leqslant D_{max}$。

此外，调度模块还必须保证实时数据流对抖动的要求，即 $D_{i+1} - D_i \leqslant J_{max}$。

结束语 本文主要讨论了 UMTS 中的 QoS 结构与功能，重点分析了一种基于包交换的 UMTS 的 QoS 体系结构与相应管理算法与机制。目前 UMTS QoS 还在不断发展和完善中，还有很多问题需要解决，如上下层之间 QoS 参数的解析和映射规程，全网络范围的资源管理和接入控制机制，支持现有异种网络之间 QoS 机制的互操作性等很多问题尚处于研究之中。由于3G 支持各种各样的业务，今后用户对通信的要求也越来越高，因此未来无线通信中的 QoS 将是一个重点。3G 的最终目标是一个全 IP 的网络，这也决定了 QoS 将是3G 的一个不可或缺的部分。所以3G 的 QoS 将是3G 研究工作的一个重点，而3G 的最终建设也必将把保证业务的 QoS 放在首位。

参 考 文 献

1 Mjögeman M. Thomasson R. Performance Simulations of the UMTS Common Packet Channel. http://citeseer.nj.nec.com/443486.html

2 Koodli R, Puuskari M. Supporting packet-data QoS in next generation cellular networks. IEEE Communications Magazine, 2001, 39(2)

3 Koh T, Levenson S, Walton T. End to end QoS considerations for UMTS. Emerging Technologies Symposium: Broadband, Wireless Internet Access, 2000 IEEE, 2000. 5

4 Chalmers D, Sloman M. A Survey of Quality of Service in Mobile Computing Environments. IEEE Communications Survey, Second Quarter 1999

5 Hultsch W. Quality of Service Support in 3rd Generation Mobile Networks. http://www.wtc2000.org/pdf/ab_006s.pdf

6 Baudet S, Besset-Mathias C, Frêne P, Giroux N. QoS Implementations in UMTS. Alcatel Telecommunications review, Q1 2001. 40～49

7 Knightly E W, Ness B. Admission Control for Statistical QoS: Theory and Practice. IEEE Network, 3/1999