公钥体系下的信任管理

王礼强，龚俭
（东南大学计算机系，南京　210096）
lqwang@njnet.edu.cn

【摘要】随着电子商业及其他应用在网上的开展，迫切需要一种在网上建立信任及分配风险的方式。公钥体系很好的解决了这一问题。本文主要介绍在公钥体系下信任管理的概念，包括：对信任的理解，风险的分析以及分派风险的各种模型（包括：订购者注册权力机构模型；证书间直接信任模型；双层信任结构模型；桥接证书机构模型；桥接认证机构模型）。文章最后对在公钥体系下信任管理各种模型的基本原则作了总结。

【关键词】公钥，信任，认证权力机构，证书权力机构。

1、引言

随着应用领域的不断扩大，安全性越来越成为影响 Internet 发展的重要因素。信任管理是安全性的一个重要方面。

在介绍公钥体系下的信任管理之前，首先阐述一下信任的概念。信任是一个早已建立的概念。有很多传统的信任关系的例子。例如：银行与帐户持有者；雇主与员工；政府与平民等等。而且之后我们可以看到传统的信任关系对建立基于公钥技术的关系是有至关重要的影响。这里所谓一个实体信任另一个实体是指第二个实体的行为是第一个实体能预见并允许的。通常第一个实体只是假定了第二个实体的行为范围。他们的信任是在这个范围之内。在电子商业中，这个范围决定公钥的使用与分布的行为。不同的信任关系表达了实体之间不同的信任程度。一个基于公钥的信任关系是为了确保第二个实体的标识说明以及双方应承担的责任。

2、基于公钥的信任关系

使用公钥技术，一个必不可少的步骤是第一个实体从第二个实体那儿得到一个公钥并且保护该公钥的完整性。得到公钥的实体叫做依靠实体。因为它依靠该公钥来保护与公钥持有者之间的信息交换。

这种关系模型图如下：

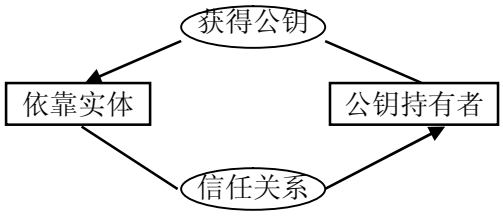

图 1

任何一个实体既可以是依靠实体，也可以是公钥持有者。但为了说明简洁起见，我把这两个角色分开讨论。

对于获得公钥这一操作而言，我们必须保证公钥的两个安全属性：

（1）真实性和完整性。也就是说该公钥的声明持有者与真正公钥持有者是相同的，且没有被修改过。

（2）明确性。它的含义是：依靠该公钥的实体对该公钥使用范围的理解与公钥持有者的理解相同。

这些安全属性只有通过已建立的信任关系才能确保其可信性。因此，似乎出现了一个矛盾：一个信任关系不能建立在无任何信任关系的基础之上。其实这也是与实际情况相符的。例如：公司的业务员，商家客户对他们的信任一般是通过对他们所在公司的信任基础上建立起来的。就公钥体系而言，我们是使用传统的信任关系作为起点来建立公钥体系下的信任关系。

一种在已有信任关系的基础上建立一种新的基于公钥技术的信任关系如下图所示。它具有完整性和明确性的特点。

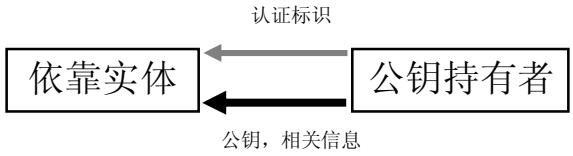

图 2

在这张图中，浅色箭头表示在已有信任关系上的操作。深色箭头表示操作的安全性是依赖于上面的。认证标记的作用是使其与公钥，相关信息相关联。它的传输是依赖于已有信任关系。而且公钥及相关信息的真实性和完整性可以使用它来保护。相关信息主要包括公钥持有者的标识描述。在很多应用中，依靠实体的目的是把公钥持有者与一定权力相关联。它使用公钥只是验证公钥持有者，并且作为赋予权力的第一环。例如：华东北网络中心开发的网络安全监测分析系统就是使用了这种方法来获得使用者的信息，然后赋予相应的访问权限。在另外一些情况下，相关信息直接暗示了公钥持有者所需的权力。

对于明确性属性，它可以通过不同的途径实现。它可以部分或隐含地被公钥的类型表示。但由于技术的原因，并不是所有的公钥都能被用于商业目的。它也可以明确地被编码到密匙使用代码中，或通过证书的政策标识符来标识。

3、信任与风险

根据 X509 的定义，公钥持有者不能按照预料进行操作这一风险是被依靠实体承担下来的。以下是一些基于公钥的信任关系而产生风险的例子：

●与密匙相关联的标识描述不正确或产生歧义。

●公钥持有者的私钥被别人发现。

●公钥持有者的默认权力已经被取消。

●公钥持有者没有充分保护好它所信任的敏感信息。

对于个体之间而言，依靠实体与公钥持有者之间有密切的关系。在这种情况下，此分配风险方式是可以接受的。因为依靠实体可以评估它的风险性并且决定是否接受。但是在电子商业中，依靠实体一般没有评估风险，决定取舍的权力或能力。在这种情况下，就需要依靠外部信任去屏蔽这个风险。一般而言，依靠实体能够找到一个适当可信任第三方来帮助分担风险。

4、分派风险模型

4.1 基本概念介绍

首先介绍以下信任第三方模型：

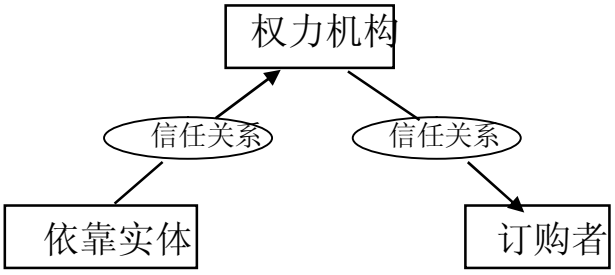

图 3 信任第三方模型

当信任是依赖于权力机构时，公钥持有者一般被称为订购者。因为一般公钥持有者希望从权力机构订购服务。我们越来越依赖电子商业系统。权力机构可能被要求承担很大一部分原先由依靠实体承担的风险。为了不使一个权力机构承担过多的风险，它需要有一种分派风险的机制。

对于这里权力机构而言，它可以分为两类。一类是认证权力机构，另一类是证书权力机构。当权力机构与依靠实体及权力机构与订购者有传统的信任关系，并且基于公钥的关系只直接存在于依靠实体与订购者之间时，这个权力机构就被称为认证权力机构。当权力机构与依靠实体，权力机构与订购者之间建立的是基于公钥关系时，权力机构被称为证书权力机构。

认证权力机构的信任关系模型图：

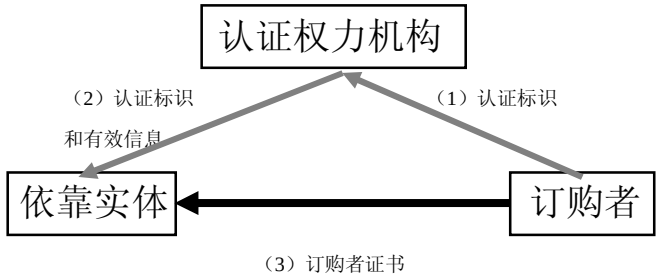

图 4 认证权力机构的信任关系模型

该流程是：

（1）订购者向认证权力机构提供认证标识符。

（2）正确注册之后，权力机构把认证标识与可用有效信息传给依靠实体。

（3）依靠实体可以直接从订购者处获得他的公钥并且用认证标识来确认其真实性。

证书权力机构的信任关系模型图：

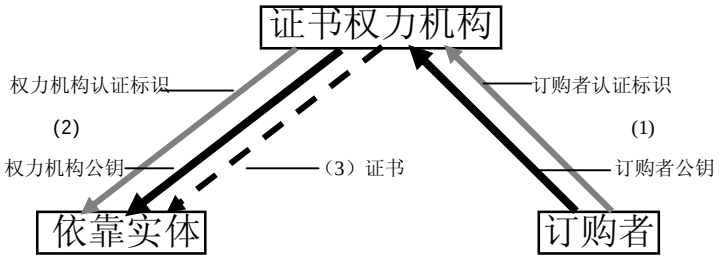

图 5 证书权力机构的信任关系模型

其步骤如下：

（1）订购者的公钥通过一种安全协议传给证书权力机构。

（2）该证书权力机构的公钥也通过这种安全协议传给依靠实体。

（3）订购者的公钥及有效信息直接通过权力机构或其它途径传给依靠实体。

对于证书的真实性，完整性和明确性是由权力机构的数字签名来保证的。这里的证书通常是指 X509 格式证书。

证书权力机构模型与认证权力机构模型相比较有以下优点：

（1）依靠实体可以用证书权力机构的证书来证明订购者证书的有效性，而认证权力机构没有这个功能。

（2）依靠实体是与权力机构直接建立关系信任关系，而不是象认证权力机构那样与订购者之间直接建立信任关系。

（3）证书权力机构可以自动取消与订购者之间的信任，然而认证机构确不行。

（4）对于证书权力机构模型有标准的协议支持，而认证权力机构却没有。

4.2、模型介绍

现在对两种权力机构的特点及基本行为方式有了一定了解，下面讨论一些适于不同情形的模型。为了方便讨论，以下用一些缩写来表示：CA－证书管理机构；AA－认证权力机构；R－依靠实体；S－订购者。箭头类型所表示的意义同上。

1）订购者注册权力机构模型

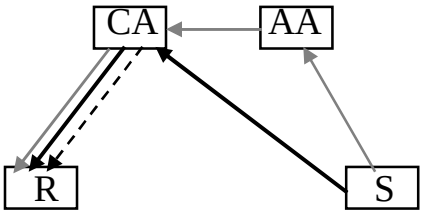

图 6 订购者注册权力机构模型

这种模型对于证书机构远离订购者时特别适用。在这种配置下，认证权力机构通常被称为订购者注册权力机构。尽管这里有两个权力机构，但证书只有一个。对于依靠实体而言，认证权力机构是不可见的。

2）证书间直接信任模型

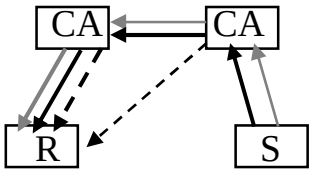

图 7 证书间直接信任模型

这种模型特别适合两个独立的组织实体之间建立直接信任关系。这里有两个权力机构和两个证书。每个涉及的权力机构对依靠实体而言都是可见的。

3）双层信任结构模型

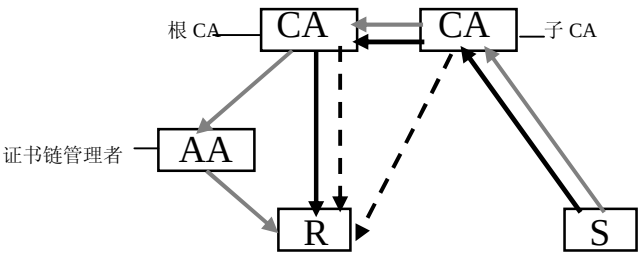

图 8 双层信任结构模型

在这里认证权力机构被称为证书链管理者。这种模型适用于子 CA 与认证权力机构分别属于不同的组织机构，它们的信任关系是通过第三方根 CA 来实现的。这里有三个权力机构，但只有两个证书。参与信任关系的认证权力机构并没有被记录在证书链中。这个证书链可以作为交易的证据。

4）桥接证书机构模型

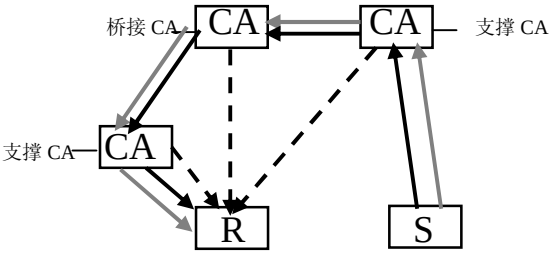

图 9 桥接证书机构模型

两个支撑证书权力机构是由两个不同的组织实体管理。它们的信任关系是通过第三方证书机构来证实的。这里有三个证书机构和三个证书。每个证书机构的作用都被记录在证书链中。

5）桥接认证机构模型

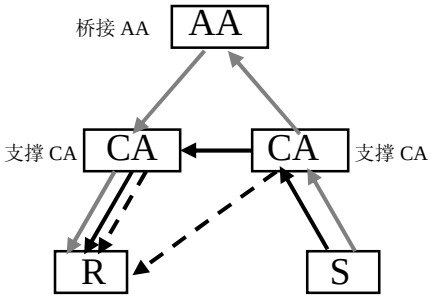

图 10 桥接认证机构模型

这个模型与桥接证书模型类似。只是第三方并不是证书机构。其中支撑 CA 间并没有传统的直接信任关系，它们的信任是通过桥接 AA 来保障。这里有三个权力机构。但只有两个证书。桥接认证机构虽然参与了整个信任过程，但在证书链中并没有它存在的记录。

5、总结

以上模型可以通过相互组合形成更为复杂的模型，但其基本思想与此类似。不同的信任模型适合不同的情形。但不管选取什么模型，依靠实体总是希望它直接依赖的机构能满足其信任要求。如果那个权力机构把风险分派到其他权力机构和订购者的话，那么这将减少它对依靠实体所承担的责任。因此，这个权力机构必须采取必要的步骤，控制其它权力机构和订购者的行为，使风险在其控制之内。

在实际操作上，信任是表现为对其直接依赖的证书机构的信任。当有认证权力机构参与时，它对依赖实体而言是不可见的。尽管有很大一部分风险被认证权力机构承担下来，但是依赖实体看上去只是信任那些可以直接得到公钥的证书机构。

参考文献

【1】 ITU-T Recommendation X.509(1997E):Information Technology, Open system interconnection-The Directory authentication framework 1997 年

【2】Internet draft certificate policy and certificate practice framework

【3】龚俭:《计算机网络安全概论》 1997 年 10 月

【3】Netscape Corp: “Security White Paper”1998 年

Trust Management in PKI

Wang LiQiang GongJian

(SouthEast University Computer Science Department, Nan Jing 210096)

【Abstract】With the wide use of electronic commerce and other application in internet, the need to establish a mechanism for trust and risk distribution has been greatly increased. Public key infrastructure model can solve this problem. The main concern of this article is to clarify the concept of trust management in PKI including trust, risk and five kinds of risk distribution models. In the last part of the article, I give a summary of basic principles of trust management in PKI. [1]

【Keywords】public-key, trust, authentication authority(AA), certificate authority(CA)

王礼强 硕士研究生 主要从事网络安全研究