PKI技术及评估

张春起 李新 杨义先 (北京邮电大学信息安全中心 100876)
游林 (大连理工大学应用数学系 116023)

摘要：PKI作为公开密钥基础设施，为基于网络的新型互联网金融服务和机密信息的传输等提供一个安全可靠的网络环境。本文简要介绍PKI的基本概念、主要功能以及如何评估一个实用PKI系统。

关键词：数字证书签名验证信息安全

1 PKI概述

PKI(Public Key Infrastructure)的中文名称为：公钥基础结构。它是一个利用现代密码学中的公钥密码技术在开放的Internet网络环境中提供数据加密以及数字签名服务的统一的技术框架。

PKI技术的主要目的是管理在开放Internet网络环境中使用的公开密钥和数字证书，从而为一个机构或集团建立一个相对安全和值得信赖的网络环境。PKI包括两个主要的安全技术：公钥加密技术、数字签名和验证技术。

公钥加密是完成信息保密性和访问控制的有效技术，它保证了用公钥加密后的数据，如果没有提供相应的私钥来解密的话，窃密者即使获得密文也难以知晓其中的内容。数字签名和验证则保证了网络通信之前相互认证双方的合法性、通信过程中信息完整性和通信结束之后防止双方相互抵赖的有效技术。这些功能的获得，就要通过PKI的密钥管理技术来实现。

2 PKI的主要功能

PKI的功能包括很多方面，主要有签发、存储与检索数字证书；签发、存储与检索证书作废表；完成密钥生成、密钥备份、备用和恢复、密钥作废与更新、密钥归档等；完成基于策略的证书校验和审计等。

2.1 RA功能

RA即是Registeration Authority，我们常说的“注册管理中心”。它主要完成收集用户信息、审核用户身份的功能。这里指的用户是：指将要向认证中心(即CA)申请数字证书的客户，可以是个人，也可以是集团或团体、某政府具体机构等。

注册管理一般都是由一个独立的注册机构(即RA)来承担的。它接受用户的注册申请，审查用户的申请资格，并决定是否同意CA给其签发数字证书。注册机构并不给用户签发证书，而只是对用户进行资格审查。因此，RA可以设置在直接面对客户的业务部门，如银行的营业部、机构认证部门等。

当然，对于一个规模较小的PKI应用系统来说，可把注册管理的职能由认证中心CA来完成，而不设立独立运行的RA。但这并不是取消了PKI的注册功能，而只是将其作为CA的一项功能而已。PKI国际标准推荐由一个独立的RA来完成注册管理的任务，可以增强应用系统的安全。

2.2 CA功能

CA即是Certificate Authority，我们常说的“认证中心”。在PKI体系中，CA扮演了非常重要的角色。这是整个PKI体系中各方都承认的一个值得信赖的公正的第三方机构。正因为CA是一个各方都信任的机构，所以它签发的数字证书也就值得大家信任，而相应的数字证书所代表的通信双方的身份也就可以信任。

(1) 签发证书。为合法的申请者签发数字证书，可以说是CA甚至是整个PKI的核心功能。如果没有CA签发证书，PKI的整个信任体系也就无从建立。一张数字证书的主要内容包括：证书版本号、证书序列号、签名算法、证书签发机构、证书的有效期、证书用户名、证书公钥信息和证书扩展项以及CA对证书的数字签名值等。正是由于数字证书中存在CA对证书的数字签名，因此对证书中任何内容的改动都可以被发现。证书中CA的签名保证了证书信息的完整性，它可以很容易地被校验。因此，证书的安全也就有了坚实的保证，它可以公开发布。

(2) 作废证书。在数字证书的有效期结束之前，由于某种原因需要提前停止使用时，就需要作废数字证书。例如，证书的所有者可能改变了姓名、单位，或者其私钥被破坏等，都需要提出对证书的作废处理。

经过CA作废的证书不再值得依

赖。因此，用户在接受通信对方的证书时，必须校验对方证书的有效性，包括CA的签名是否正确，证书是否被作废处理等。PKI中检查证书是否作废的常用方法是检查证书作废表(CRL)。CA在作废处理证书时产生新的证书作废表，它可以以一定的格式公布于众。用户可以方便地查询到证书作废信息。这里要注意，作废的证书也要经过认证中心的数字签名，以确保可信任。

2.3 证书管理

证书管理包括的内容十分广泛，大致可分为证书的存取、证书链校验，以及交叉认证等方面。

(1) 证书的存取。数字证书由CA签发后，必须通过一定的渠道进行发布，才能广为人知，并加以利用。PKI中使用证书存取库来发布和存放所有用户的数字证书，并提供目录服务。当然，证书存取库中还存放有证书作废表等信息。目前，大多数数字证书选择LDAP(轻量目录访问协议)服务器作为证书存储库，供用户查询和下载。

(2) 证书链校验。在PKI体系中，CA是有层次结构的。n级PKI体系中，在信任体系的最高层是根认证中心(RootCA)，一般它只有一个，并且自己给自己签发证书。Root CA的下级是二级认证中心(Second CA)，它可以有多个，其证书由根认证中心签发。二级认证中心的下级是三级认证中心(Third CA)，它负责为四级认证中心(Fourth CA)，而它本身的证书则由二级认证中心签发，…，直到n级认证中心(nth CA)，它负责为最终用户签发证书，而它本身的证书则由n-1级认证中心签发。当然，这里并不否认各级CA中心可签发用户证书的可能性。

从证书的层次上看，由下到上构成了一条证书链。注意，这里的每一级CA，都存在与之对应的RA。

假设在一个2级PKI应用系统中，用户A的证书由二级认证中心C签发，而用户B的证书由二级认证中心D签发。如果用户A不信任通信对方用户B，它就需要校验用户B的数字证书。这时它就需要首先获取为用户B签发证书的二级认证中心D的证书，并利用其公开密钥校验用户B的证书上的数字签名。如果用户A对用户B的二级认证中心D的身份也不信任，它还要继续获取为二级认证中心D签发证书的根认证中心的证书，并利用其公开密钥校验二级认证中心D的证书的数字签名。根认证中心的证书是自签名的，可以自行验证。

(3) 交叉认证。利用交叉认证技术可以扩展CA的信任范围，它允许不同信任体系中的认证中心建立起可信任的相互依赖关系，从而使各自签发的证书可以相互认证和校验。

交叉认证包括了两方面的内容：首先，两个CA建立起信任关系。这就要求双方安全地交换用于校验签名的公开密钥，并利用自己的私有密钥为对方签发数字证书，从而双方都拥有了交叉证书。其次，利用CA的交叉证书校验最终用户的证书。这对用户来说，就是利用本方CA的公钥来校验对方CA的交叉证书，从而决定对方CA是否可信；再利用对方CA的公钥来校验对方用户的证书，从而决定对方用户是否可信。

需要注意的是，交叉证书也是可以作废的，因此在进行交叉认证时，必须同样需要校验交叉证书是否已经作废。

2.4 密钥管理

在PKI体系中，密钥的管理主要包括密钥生成、密钥更新、密钥备份和恢复、密钥销毁和归档处理等。

PKI技术要求每个用户拥有两个公私密钥对。其中一对密钥用于数据加密和解密，另一对密钥用于数字签名和校验签名。这种要求主要是为了支持数字签名的不可否认性。但是，它们在密钥管理中的要求并不一样。

(1) 密钥产生。用于加密/解密目的的密钥对，可以在一个可信的第三方机构产生，也可以在客户端产生。如果在异地产生该密钥对，必须能够保证将其安全地传输到客户端，供客户使用。

用于签名/校验的密钥对，必须在客户端产生。在一些情况下(如客户端没有能力产生密钥对)也可以在一个可信的第三方机构产生。但当用户获得该密钥对后，第三方机构必须毁销该密钥对中用于签名的私钥，并且该私钥只能由用户本身唯一拥有，严禁在网络中传输，或存放于网络中的其他地方。但用于校验签名的公钥可以在网络中传输，还可以随处发布。

(2) 密钥备份和恢复。PKI要求应用系统提供密钥备份与恢复功能。当用户的密钥访问口令忘记时，或存储用户密钥的设备损坏时，可以利用此功能恢复原来的密钥对，从而使原来加密的信息可以正确解密。

但并不是用户的所有密钥都需要备份，也并不是任何机构都可以备份密钥。可以备份的密钥是用于加密/解密的密钥对，而用于签名/校验的密钥对则不可备份，否则将无法保证用户签名信息的不可否认性。用于签名/校验的密钥对在损坏或泄露后，必须重新产生。另外，可以备份密钥的应该是可信的第三方机构，如CA、专用的备份服务器等。

(3) 密钥更新。密钥的使用是存在有效期的。当密钥到期时，用户应到本地RA中心申请并更新证书，旧的证书将被废止。

(4) 密钥归档。当用于加密/解密的密钥对成功更新后，原来使用的密钥对必须进行归档处理，以保证原来的加密信息可以正确地解密。但用于签名/校验的密钥对成功更新后，原来密钥对中用于签名的私钥必须安全地销毁；而原来密钥对中用于校验签名的公开密钥则可以进行归档管理，以便将来对原来的签名信息进行校验。

另外，PKI的密钥管理总体来说应该是自动的，并且是对用户透明的。

要强调的是，为确保PKI体系的安全性，根证书和下属各级证书的私钥须确保安全、具有严格的备份手段，以便遭破坏后恢复。要注意，根证书的备份过程，必须多人同时参与，任何一个管理员都不能独立完成备份过程，另外，根证书和下属各级证书的须有备用证书，以在紧急情况下使用。

3 实用PKI系统的评估

PKI技术日趋成熟，产品丰富多彩，但多数PKI系统的实用价值值得商榷，我们认为：一个实用的PKI系统必须具有满足下面属性：

(1) 安全可靠性：包括系统安全、数据安全和通信安全。PKI系统必须要防止来自系统内部和来自系统外部的威胁，保证系统不崩溃，防止信息窃取，要有足够的能力防止恶意的攻击。

(2) 先进性：信息技术的发展十分迅速，在综合考虑性价比的前提下，及时了解新技术，使用先进的技术、设备和算法，使目标PKI系统更先进、更完善。

(3) 标准性：PKI系统应支持多种平台和应用，支持多种证书类型以及支持多种证书发行和管理协议，满足交叉认证和不同PKI产品的系统集；PKI系统应遵循相应的国际(如PKCS#f1～PKCS#15协议标准等)，严格地说，PKI技术和标准还处在发展阶段，很难预计以后PKI会使用或需要某种确定的东西。因而，为了保护你的投资和防止未来的互操作出现问题，选择一种完全开放的、建立在最通用和先进标准上的PKI是很重要的。

(4) 扩展性：随着组织对PKI的使用和依赖性都不断增长，PKI应该能适应这种需求。开始，PKI可能只支持一种应用，但它必须能够支持以后能得到的应用。它必须能够通过增加额外的CA和RA来支持不断增长的证书需要。另外当PKI扩展后会包含新的服务，需要各种证书的类型和注册的机制。

(5) 灵活的无缝组合：PKI的各个组成部分的互操作性是很重要的，因为有可能它们不都是由一个提供商提供的。比如说，CA可能必须和一个已经存在的系统有接口，如果一个组织中已经安装了目录服务器的话，PKI必须使用开放的标准的接口，比如LDAP和X.500(DAP)，确保它能和所有的兼容标准的目录服务工作。另外，许多组织已经选择了智能卡和硬件安全模块(HSM)的供应商，所以，使用开放的标准的接口，比如PKCS#11(Cryptoki)，PKI就具有和广泛的范围内的安全令牌一起工作的能力。因此，作为安全的一个核心部分，PKI系统能够无缝地组合到的多个业务应用系统中去。

(6) 易操作性：PKI系统必须是容易操作和透明的，即PKI应该使非技术人员，比如商务管理人员可以很自信地操作它，使他们不需要了解PKI系统是如何管理密钥和数字证书，通过应用程序提供的简单图标和对话框，就能实现数据加密和数字签名等服务。虽然PKI使用的原理可能很复杂，但它的管理不应该很复杂。这些操作人员不需要处理复杂的加密算法，密钥和签名。应该只是点一下图标，剩下的都让应用软件去做了。因此，界面应该是图形化并很直观地帮助完成管理任务。

(7) 经济原则：体现实用性，系统提供一个高性能价格比。大而全和高精尖并不是成功认证系统的衡量标准。事实上许多失败的系统正是由于盲目追求高新技术而忽视了其实用性，盲目追求完善的系统而忽视了本单位的技术水平、管理水平和人员素质。

(8) 可维护性：整个系统应具备良好的可维护性。PKI系统的软、硬件系统都具有良好的模块化结构，保证系统设计的合理性，配置相关的管理手段。

(9) 审计功能：所做的任何事情都要有记录。每个条目都要表明时间和签名。即在安全统计中具有较完备的审计功能。

(10) 符合国家有关法律法规：PKI系统完全符合国家关于密码产品的相关法律、法规。■

参考文献

1 冯登国等译，公开密钥基础设施－概念、标准和实施，人民邮电出版社，2001。

2 Thayer, R, N. Doraswamy, and R. Glenn. IP Security Document Roadmap. Inernet Request for Comments 2411. 1998-11。

3 PKI技术及其标准 http://toppage.topcool.net/sec_pki.htm。