PKI在电子信息安全中的有效应用

刘　帆
成都信息工程大学，四川成都　610000

摘　要　随着互联网信息技术的不断发展，电子信息在日常工作生活中的应用愈加的频繁，为了应对日益突出的网络安全问题，PKI技术逐渐在电子信息安全中推广开来。PKI，即公钥基础设施，是当前网络安全建设中的一项核心技术，也是目前信息安全领域研究关注的焦点问题之一。本文通过对PKI技术的简单介绍，探究骑在电子信息安全中的有效应用。

关键词　PKI；电子信息安全；应用
中图分类号　TP39　　**文献标识码**　A　　**文章编号**　1674-6708（2015）145-0080-02
DOI:10.16607/j.cnki.1674-6708.2015.16.050

由于因特网逐渐在世界范围内普及，人们在交流过程中使用因特网的次数日渐频繁，使得电子商务也逐渐推广开来，但是由于网络环境的复杂性，致使电子信息安全问题也日渐突出，而PKI技术能够更好地解决在电子信息交换过程中的安全问题，使得电子信息的安全得到有效的保障。

1 电子信息安全问题

伴随着电子商务信息的不断发展，其中的信息安全问题也逐渐出现，主要有：在网络传输过程中大量保密信息被窃取；在网络交易的过程中，交易信息容易被中途篡改或者是发布虚假的交易信息；电子信息交换双方的身份信息的正确性得不到确认；当双方电子信息交易完毕之后，另一方有可能出现否认的现象等，这一系列的安全问题直接影响着电子商务信息的进一步发展，因此，解决电子信息的安全问题，成为电子信息发展的当务之急[1]。

2 PIK技术的内涵

为了解决电子信息交换过程中的安全问题，PKI技术应运而生。PKI，即公钥基础设施，这是网络密码技术逐渐发展过程中产生的一项技术，PKI通过借助公共密钥技术，搭建一个技术平台，从而为网络电子信息的安全提供一定的规范，事实上，PKI就是由一整套软硬件系统以及安全策略相组合而形成的一个集合，其中最为基础的一项元素就是数字证书，有了数字证书，PKI平台才能够发挥出其对信息安全的控制作用。而这一平台是通过网络中真实存在的CA，即信息传输认证中心，根据网络中信息使用者的分布状况，不断发送数字证书，从而最终到达用户端。

3 数字证书

数字证书是一种证明信息所有者的电子性文件，一般由CA进行发放，其主要含有的信息与公开密钥相关。数字证书能够保证在电子信息传输过程中的保密性以及完整性，同时，它能够对信息所有者的身份进行鉴别，从而保证其身份的正确性，从而避免电子信息中出现的安全隐患。除此之外，数字证书还能够有效的防止电子信息在进行交换中出现的恶意篡改现象，在数字证书的监督之下，破坏信息完整性的违规操作无法轻易进入到电子信息交换的环节，而一旦电子信息到达接收方，再通过签名以及身份验证等环节后，电子信息就拥有了唯一的所有权，同时也具备了不可否认的特性[2]。

4 PKI平台的组成

一般来说，国际上所使用的PKI平台主要是由软硬件系统、组策略、数字证书以及CA等组成。

4.1 组策略

组策略一般是在保持软硬件系统稳定的基础之上，然后根据国际上普遍所使用的密码准则，在PKI平台的操作系统当中建造出系统的安全指导方案或者建立一个相应的密码系统。

4.2 CA

如果要想有效的管理公共密钥，就应当有一个与之相应的认证机构在其中发挥出相应的作用，而CA，作为数字证书进行认证的一个机构，其主要是借助数字证书的发送以及其对数字证书的相关规定来对公共密钥进行管理。CA作为保证PKI平台照常运行的一个基础性环节，若缺少了对数字证书的有效监管，那就会致使电子信息的安全得不到控制及保障。

5 PKI在电子信息安全中的应用

5.1 身份验证

由于信息网络环境之中的用户数量众多，要想对这数以亿计的用户进行身份信息的验证是一项不小的工程，因此，为了能够有效地统计网络用户的信息，相关的技术人员通过长期的研究开发，最终确定出了使用公用密钥和数字证书，通过一定的规范来对网络环境中的用户进行身份的验证。PKI平台在利用这一方式对网络用户进行身份验证之时，需要借助第三方的认证力量来实现，而这第三方的力量就是CA。CA通过借助RA实现了对数据交换用户相关信息的收集和整理，然后再把与用户相关的标志性的信息与公用密钥进行绑定，对于满足相关认证条件的信息用户，CA统一对其发送特定的数字ID，而发送的这种特定的数字ID本身就拥有唯一性，避免了伪造的现象，当用户具有了这一数字ID之后，就可以开始更进一步的数据信息的交流。

就目前而言，网络电子商务在进行信息交流的过程中，使用的较为普遍的支付宝以及财付通等都实现了身份验证这一功能[3]。除此之外，鉴于在进行网络电子商

务的过程中，用户对于密码等的相关要求都比较高，现实生活中的部分网络交易性质的网站都借助 CA 建立了双重甚至是多重的身份信息验证系统，也就是说用户要想在网络上进行资金的支付，就必须要使用两个甚至是多个数字证书才能够进行有效的支付操作，从而保证了用户在电子信息交换过程中的私密性，也使用户身份信息的验证得到了进一步的强化。

5.2 电子信息的完整性

由于网络环境十分的复杂，在开放的网络环境当中，存在有电子信息被第三方非法截取甚至篡改的现象，直接影响了电子信息的完整性，而只有保证网络电子信息传输中的完整性，才能够使得电子信息的交换存在着意义，因此，这就要求针对开放的网络环境，必须要加强对电子信息完整性的有效控制，从而避免电子信息被截取或者篡改，确保电子信息的安全。针对这一的要求，PKI 平台实现了数字信息检索技术的应用，数字信息检索技术主要是针对电子信息之中具有标志性的相关信息元素进行必要的编码，从而使之形成一种较为特别的电子信息摘要码。摘要码主要应用的是一种数字函数的技术，通过把电子信息文件之中的关键性元素转化成与之相对应的数字编码，然后由发送方发送给接收方，而接收方则根据相应的规则对编码进行解析，从而得到完整的电子信息，这种方法能够有效地检验电子信息的完整性，从而保证了信息的安全。

5.3 电子信息的不可否认性

PKI 平台除了具有身份验证、保证信息完整及其私密性之外，其所具有的数字签名技术也是电子信息交换中的一种有效凭证，能够证明电子信息进行传递的时间、发送以及接收电子信息双方的资料，一旦电子信息交换双方发生纠纷，这些证明信息都可以成为必要的参考材料，从而使得与信息有关人员都不能推卸其应担的责任。

6 结论

随着互联网信息技术的不断发展以及普及，越来越多的人都使用电子信息进行交流沟通，而 PKI 作为保障电子信息安全的有效手段，逐渐在信息时代中推广开来，发挥的作用也越来越大，就目前而言，PKI 是当前最为成熟的一项电子信息安全保证体系，通过 PKI 平台技术能够有效地解决网络环境中用户的身份信息验证难问题，保证了电子信息在进行交流过程之中的安全保密性，避免了电子信息的中途篡改以及泄露现象，从而为电子信息的交流提供了强有力的安全保障。

参考文献

[1]沙非.PKI在电子信息安全中的有效应用[J].中国西部科技，2011，10（22）：16-17.

[2]负强.PKI在电子信息安全中的应用[J].中国高新技术企业，2011（3）：61-62.

[3]苏命峰.PKI在信息安全中的应用与实现[J].计算机时代，2009（7）：15-17.

（上接第77页）

但过于平正缺乏明暗之分，缺乏立体效果，容易使主体和背景、前景混淆起来。侧光拍摄时，画面会产生阴影，显现明暗的线条，使画面层次丰富，具有立体感，是理想的光线之一。逆光拍摄时使主体与背景、前景截然分开，物体与物体之间都有明显的光的界线，不会使主体与背景重叠混合成一片。高光拍摄时除了能表现由上到下的阴暗层次外，无法表现物体的质感，这种光线不是拍摄的理想光线，尽量少用。散射光拍摄时不能产生明暗的层次和线条，在取景时尽量缩小景别，采用中景或局部场面，才能获得较为清晰的效果。

第四，充分运用摄影的技术技巧，使画面表现形式更新颖、生动和艺术性。

摄影作为一门艺术，力求创新，突破视觉规律，一张思想性强、艺术性高的摄影作品，必须有高超的摄影技术手段和摄影艺术素养来保证，不仅让受众者为其内涵所震撼，也要被表现形式新颖、生动所感染。在越来越追求真善美的今天，合理地在摄影中贯穿艺术性的原则与元素，能够极大地提升摄影作品的阅读效果，使作品更易被理解和接受，从而起到更好的社会效果。

大众普遍采用的方法有虚化法和动感法。虚化法就是利用长焦距和大光圈，将主体以外的部分虚化，以虚托实，虚实相衬，将会产生很好的画面效果。虚化取决于镜头焦距的长短，光圈的大小，背景器物距离主体物的远近等等。镜头焦距越长，光圈开得越大，背景器物距离主体物越远，背景影像就越虚化；反之，背景影像的虚化程度就小，甚至不虚化。动感法有控制快门速度、追随拍摄、爆炸拍摄等方法，这类照片动中有力，动中有情，动中有美。 快门速度分高速和慢速，高速拍摄能够凝固运动瞬间，固定优美的动作，展现主体的气势。慢速拍摄可以虚化动体，形成运动虚像，动感很强，同时也能表现意境，如流动的水。追随拍摄可以使运动的主体影像清晰，背景变为虚像。这种虚实结合、动静结合的画面，动感更为强烈。爆炸拍摄就是在拍摄过程中变化焦段，主体清晰，陪体在画面上变为四射的线条，给人浓重的“爆炸感”，是平淡的画面更艺术化。

总之，摄影作为一种视觉创作的途径，一些基本要求和要素某种程度上是有规可循。但要拍出好照片，与摄影者的阅历、学识、价值观等等都有关系，是一个人综合素质的具体体现。

参考文献

[1]李肖昌.摄影用光［M］.2版.长江文艺出版社.2009.

[2]龙文.数码摄影实拍技法宝典［M］.人民邮电出版社，2010.

[3]郭艳民.摄影构图［M］.中国传媒大学出版社，2011.