2006年电子新指导之PKI体系的十大风险 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/61/2021_2022_2006_E5_B9_B4_E7_94_B5_c40_61864.htm PKI（公钥设施基础，Public Key Infrastructure）是一种标准化的密钥管理平台，能为网络应用提供加密和数字签名，以及密钥和证书管理体系的服务。在几乎所有介绍PKI的书籍或文章上，我们都能看到类似于这样的一句话：使用PKI就能保证网络应用的安全。那么，PKI体系的安全性到底怎样呢？就让我们来逐一列出PKI体系的十大安全隐患： 风险1：证书持有者能被信任吗？ 在PKI中，CA总是被认为是可以信任的，并且，由CA颁发的证书的持有者也是可以信任的。但是在密码学中，CA是可以信任的，仅仅意味着CA能够妥善的保管好自身的私钥，并不意味着你有任何理由信任CA所颁发的证书的持有者（而绝大多数PKI系统甚至是不经用户许可即将可信任CA颁发证书的持有者视为可信任！）。PKI设计者的逻辑是：你已经得到一个由CA颁发的可以信任的证书，该证书告诉你持有者的姓名（或公司名等），因此你可以知道持有者是谁，而这些就是你所需要知道的全部信息。显然，这样的逻辑是不可依赖的。 风险2：你的私钥安全吗？ 在PKI体系中，证明你自己身份的唯一方法是使用你自己的私钥。但问题也就随着出现了，你保管好你的私钥了吗？存放在电脑上的私钥可能被病毒或者木马盗窃。如果你已经将私钥进行过加密处理，那么你的加密口令足够强壮吗？而一旦私钥被盗，也就相当于你的身份可以被别人随意使用，因此，这些都是不得不考虑的问题。 风险3：鉴别证书的机器安全吗？ 由于证书鉴别使用的是公钥，也

就没有任何需要保密的东西，这看来似乎是安全的。但是，证书鉴别确实需要使用一些公钥，这样，一旦攻击者成功将他的公钥添加到用于鉴别的公钥列表中，他就能自己颁发证书，并且这些证书也会被PKI体系视为合法用户。解决这个问题的唯一途径就是确保存放鉴别使用的公钥的电脑的安全性。 风险4：证书持有者就是你寻找的那个吗？ 通常，PKI证书会和持有者的姓名相联系，但在现实中，同名的人不少，光凭这一点无法判断该证书是否属于你所寻找的那个人。因此，PKI系统也添加了一些其他信息作为标识，但问题也随之而来，你对寻找的那个人有足够了解吗？同时，你知道他的证书会由哪个CA进行颁发吗？ 风险5：CA足够权威吗？ 尽管我们可以假设CA是颁发证书的权威机构，但CA是证明证书上包含内容的权威机构吗？以广泛应用的SSL为例，证书上包含的持有者姓名（通常是公司名）和DNS域名两项就有着很大的安全漏洞。首先，公司名是该公司在注册时申请的，而所有浏览器里的SSL CA都不是接受公司注册的权威机构；其次，域名也不是在CA处注册的。这样，证书持有者向CA提供的注册信息中就有足够可能性包含虚假信息，导致最终用户受骗。 