DREAMINGXIN

博客园 首页 新随笔 联系 订阅 管理

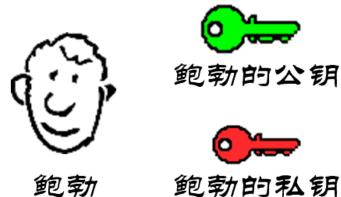
公告

随笔 - 15 文章 - 0 评论 - 2

图解公钥、私钥、证书

原文网址: http://www.youdzone.com/signature.html

1.



鲍勃有两把钥匙,一把是公钥,另一把是私钥。

2.



鲍勃把公钥送给他的朋友们----帕蒂、道格、苏珊----每人一把。

3.

昵称: DREAM.XIN 园龄: 2年10个月 粉丝: 2 关注: 1 +加关注

<		>				
日	_	=	Ξ	四	五	六
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

搜索	
	找找看
	谷歌搜索

常用链接		
我的随笔		
我的评论 我的参与		
我的参与 最新评论		
我的标签		

我的标签	
DES(2) dom4j(2) java(2) MD5(2) RSA(2) 公钥(2) 加密减密(2) 私钥(2) 证书(2) AES(2) 更多	



"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"



公钥加密

HNFmsEm6Un BejhhyCGKO KJUxhiygSBC EiC0QYIh/Hn 3xgiKBcyLK1 UcYiYlxx2lCF HDC/A

苏珊

苏珊要给鲍勃写一封保密的信。她写完后用鲍勃的公钥加密,就可以达到保密的效果。

4.



鲍勃

HNFmsEm6Un BejhhyCGKO KJUxhiygSBC EiC0QYIh/Hn 3xgiKBcyLK1 UcYiYlxx2lCF HDC/A



UcYiYlxx2lCF 私钥解密

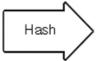
"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

5.

Fits the circulus of IGO direty Good Privary, a publishing encomposition and wave purchase for the potentions of electronic result. Show IGO was probabled consentioning to there were in Tune of 1974, the agent of open of the IGO was probabled for exemption of 8 and winning that the three weekforches shoulded for exception of 8 and winning consenses including versult in long time. On the agent was the tension of the IGO was a second to the IGO was a second to the IGO was a foreign and IGO was a f

全的,即使落在别人手里,也无法解密。

Comparison more developed in every lock in Weeld Wine 2 starting by their docies. Officially people of it is the two content to incomparison beaution tong more and in resident and the expenditive. Softway people down comparison in the executive, and some and the extent people mount given bear in the executive, and some and the extent people mount given bear in one of the energy time. Some and the prevention of whited towers of paging the following more from an of the prevention to severe the old with rate in the region with the proof and to severe the old with rate in the region with the proof and people has the basis or some to place of pagingspage.



鲍勃收信后,用私钥解密,就看到了信件内容。这里要强调的是,只要鲍勃的私钥不泄露,这封信就是安

Digest

鲍勃给苏珊回信,决定采用"数字签名"。他写完后先用Hash函数,生成信件的摘要(digest)。

6.

随笔分类

AES(1) BASE64(1) Dom4j(2) java加减密(9) MD5(1) RSA(1) SHA(1) URL编码(1) xml(1) 对称加密(2) 摘要算法(2)

随笔档案

证书(2)

2017年12月 (2) 2017年11月 (13)

文章分类

java加减密

最新评论

- 1. Re:Dom4j中使用asXML方法之 节点自闭和问题 可以用,谢谢
 - --殁舞
- 2. Re:Dom4j中使用asXML方法之 节点自闭和问题 根本就不管用
 - --暮色听雨声

阅读排行榜

- 1. CA证书下载以及导出公私钥教程 (7538)
- 2. 常见数字证书类型(3693)
- 3. openssl实现公私钥证书生成以 及转换(3411)
- 4. Dom4j解析xml(3207)
- 5. 图解公钥、私钥、证书(2922)

评论排行榜

1. Dom4j中使用asXML方法之节 点自闭和问题(2)





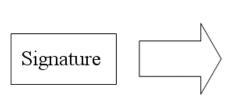
Signature

推荐排行榜

- 1. 图解公钥、私钥、证书(2)
- 2. Dom4j中使用asXML方法之节 点自闭和问题(1)
- 3. 常见数字证书类型(1)

然后,鲍勃使用私钥,对这个摘要加密,生成"数字签名" (signature) 。

7.



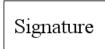
The this common of 100 d period could historically a publishing anotypical method processing of the processing of inchronau could school processing of inchronau could school processing and processing of the could stiff of

congraices ment de entioped in meter lond in Weeld What 2 activity by mich clother. Children propried Crit of this were constructively seen and ting years and in michaelm and the expending. Since people and another in the constructive and the expending. Since people above computers in the constructive and an one of that excit leavy people would a mark have used for exception. Decay of the greatment of the constructive and the expending of the constructive and the constructive and the constructive and the constructive constructive and constructive to the constructive and the constructive and the constructive constructive and constructive to the constructive co

Signature

鲍勃将这个签名,附在信件下面, 一起发给苏珊。

8.

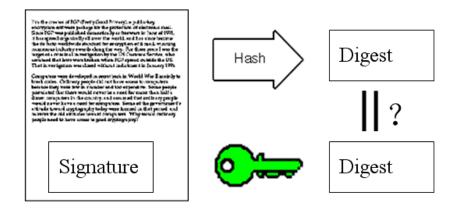




公钥解密

Digest

苏珊收信后,取下数字签名,用鲍勃的公钥解密,得到信件的摘要。由此证明,这封信确实是鲍勃发出 的。

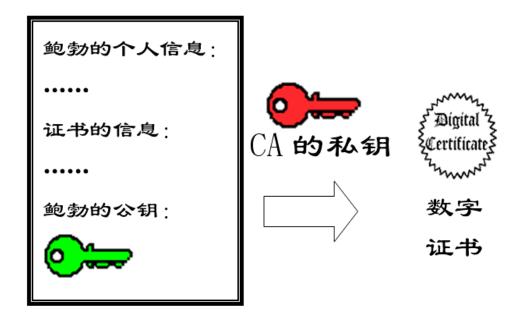


苏珊再对信件本身使用Hash函数,将得到的结果,与上一步得到的摘要进行对比。如果两者一致,就证明这封信未被修改过。

10.



复杂的情况出现了。道格想欺骗苏珊,他偷偷使用了苏珊的电脑,用自己的公钥换走了鲍勃的公钥。此时,苏珊实际拥有的是道格的公钥,但是还以为这是鲍勃的公钥。因此,道格就可以冒充鲍勃,用自己的私钥做成"数字签名",写信给苏珊,让苏珊用假的鲍勃公钥进行解密。

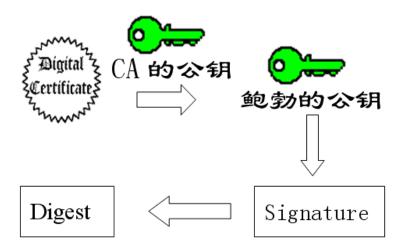


后来,苏珊感觉不对劲,发现自己无法确定公钥是否真的属于鲍勃。她想到了一个办法,要求鲍勃去 找"证书中心"(certificate authority,简称CA),为公钥做认证。证书中心用自己的私钥,对鲍勃 的公钥和一些相关信息一起加密,生成"数字证书"(Digital Certificate)。

12.



鲍勃拿到数字证书以后,就可以放心了。以后再给苏珊写信,只要在签名的同时,再附上数字证书就行了。

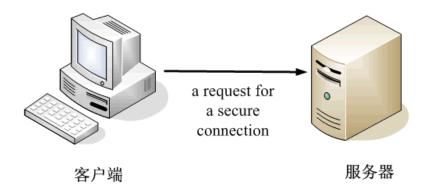


苏珊收信后,用CA的公钥解开数字证书,就可以拿到鲍勃真实的公钥了,然后就能证明"数字签名"是否真的是鲍勃签的。

14.

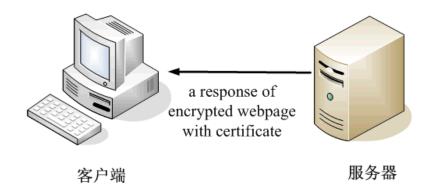


下面,我们看一个应用"数字证书"的实例:https协议。这个协议主要用于网页加密。

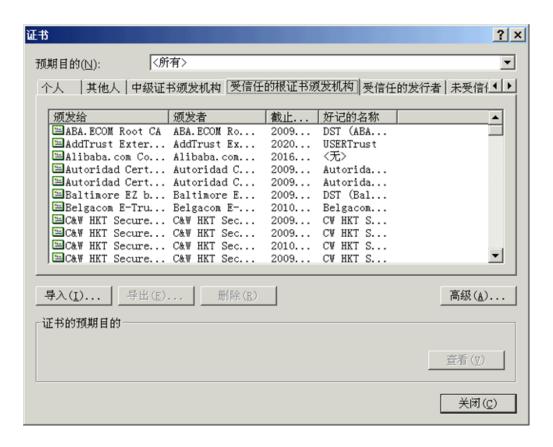


首先,客户端向服务器发出加密请求。

16.



服务器用自己的私钥加密网页以后,连同本身的数字证书,一起发送给客户端。

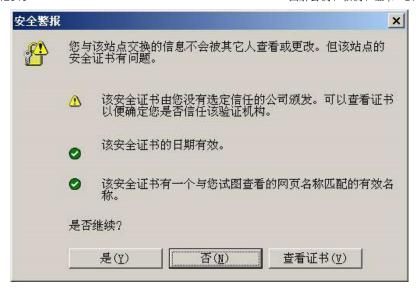


客户端(浏览器)的"证书管理器",有"受信任的根证书颁发机构"列表。客户端会根据这张列表,查看解开数字证书的公钥是否在列表之内。

18.

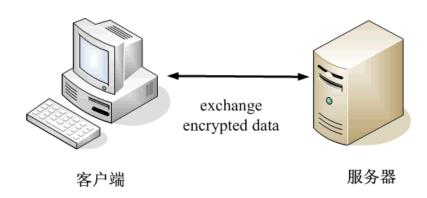


如果数字证书记载的网址,与你正在浏览的网址不一致,就说明这张证书可能被冒用,浏览器会发出警 告。



如果这张数字证书不是由受信任的机构颁发的,浏览器会发出另一种警告。

20.



追梦若冷 就用希望去暖

分类: java加减密

标签: 公钥, 私钥, 证书



«上一篇: Dom4j中使用asXML方法之节点自闭和问题

» 下一篇:加密与签名的区别

posted @ 2017-11-29 09:43 DREAM.XIN 阅读(2922) 评论(0) 编辑 收藏

2

刷新评论 刷新页面 返回顶部

0

注册用户登录后才能发表评论,请 登录 或 注册,访问网站首页。

【推荐】超50万C++/C#源码: 大型实时仿真组态图形源码

【前端】SpreadJS表格控件,可嵌入系统开发的在线Excel

【活动】"魔程"社区训练营技术沙龙——React 前端开发专场

【推荐】程序员问答平台,解决您开发中遇到的技术难题

相关博文:

- ·公钥和私钥
- · 数字证书--图文解说
- · 轻松理解数字签名和数字证书的关系
- · 数字签名到底是什么鬼?
- ·数字签名和数字证书

Copyright ©2019 DREAM.XIN