

SSL安全证书-概念解析

一、关于证书

数字证书是一种认证机制。简单点说，它代表了一种由权威机构颁发授权的安全标志。

由来

在以前，传统网站采用HTTP协议进行数据传输，所有的数据几乎都用的明文，很容易发生隐私泄露。为了解决安全问题，大家开始考虑采用加解密方案，于是乎诞生了公钥加密(非对称加密)及签名算法。浏览器从服务端得到公钥，经过协商并生成动态密钥，此后所有的请求响应都基于动态密钥加密解密。然而对于浏览器而言，是不是所有声称了 HTTPS 的服务器都值得信任呢。答案是否定的，服务器必须提供一个凭证以证明自己值得信任，于是乎这就有了证书，通常的证书里面则包含了公钥。浏览器与服务器进行加密数据传输的前提是服务器证书受到信任，即存在于浏览器的受信任证书列表中。

二、PKI - 公钥基础设施

Public Key Infrastructure，是基于公开密钥技术所构建的，用以解决网络安全问题的通用基础平台。其服务范围包括公钥管理、提供认证、加密、完整性和可追究性服务。

PKI 几乎可以代言整个公钥技术体系标准。从概念上，PKI 涵盖了 PMI（权限管理），然而实质上 PKI 不仅如此，目前只要是基于公钥技术实现网络安全的所有协议、组件、服务等都从属于 PKI，包括上述的证书。

PKI 的关键元素：

- 1 数字证书 Certificate
- 2 证书签署机构 CA 及批准机构 RA

公告



美码师，老码农一枚，喜欢聊聊代码，唠唠职场故事，爱技术也爱生活，欢迎关注我的公众号

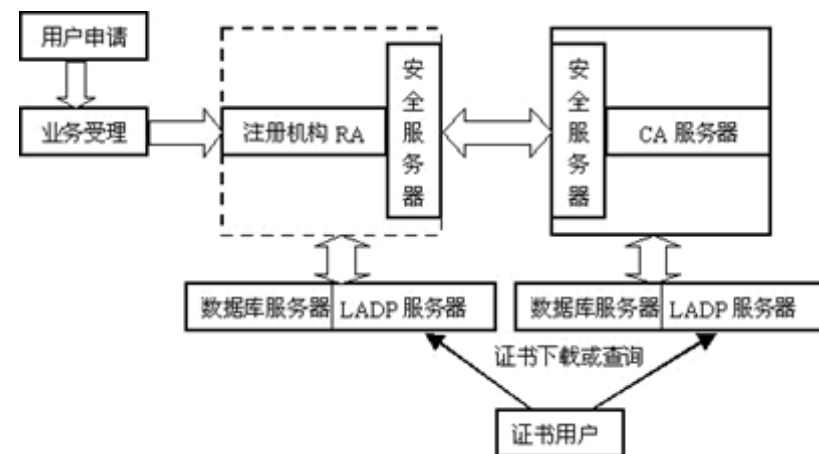


昵称：美码师
园龄：8年5个月
粉丝：90
关注：7
+加关注

<		2019年6月						>
日	一	二	三	四	五	六		
26	27	28	29	30	31	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		

三、CA - 证书授权中心

Certificate Authority, CA 是负责发放并管理数字证书的第三方权威机构, 它负责管理 PKI 体系中的所有组织、个人、以及他们持有的数字证书, 将用户的公钥及用户的其他信息捆绑在一起, 在网上验证用户的身份。CA机构的数字签名使得攻击者不能伪造和篡改证书。



CA 的层级结构

CA 建立自上而下的信任链, 下级 CA 信任上级 CA, 下级 CA 由上级 CA 颁发证书并认证
如github的证书层级:

CA 的功能:

证书颁发: 接收、验证及受理用户(包括下级认证中心和最终用户)的数字证书的申请。

证书更新: 认证中心可以定期更新所有用户的证书, 或者根据用户的请求来更新用户的证书

证书查询: 查询当前用户证书申请处理过程; 查询用户证书的颁发信息, 这类查询由目录服务器LDAP来完成

搜索

找找看

常用链接

我的随笔

我的评论

我的参与

最新评论

我的标签

随笔分类

0.JAVA技术(39)

1.架构设计(3)

2.安全技术(9)

3.前端技术(2)

4.测试技术(2)

5.数据库中间件(21)

7.工具技巧(9)

8.构建技术(5)

9.基础原理(2)

O.开放平台(3)

P.行业相关(1)

S.敏捷管理

Z.心得杂谈(9)

随笔档案

2019年5月 (2)

2019年4月 (4)

2019年3月 (7)

2019年2月 (2)

2018年12月 (2)

2018年11月 (6)

2018年9月 (3)

证书作废：由于用户私钥泄密等原因，需要向认证中心提出证书作废的请求；证书已经过了有效期，认证中心自动将该证书作废。认证中心通过维护证书作废列表 (Certificate Revocation List,CRL) 来完成上述功能。

证书的归档：证书具有一定的有效期，证书过了有效期之后就将作废，但是我们不能将作废的证书简单地丢弃，因为有时我们可能需要验证以前的某个交易过程中产生的数字签名，这时我们就需要查询作废的证书。

来源：

四、Certificates 数字证书

主要构成

1. 申请者信息；
2. 申请者公钥；
3. 签发机构CA及数字签名
4. 证书有效期

证书标准

1.
x.509 是PKI 体系中最基础的标准，它最先定义了公钥证书的基本结构：
SSL公钥证书
证书废除列表CRL(Certificate revocation lists)
2.
PKCS#12
windows 平台及 mac平台使用的证书标准，通常使用 pfx/p12 作为文件扩展名，
该标准在X509的基础之上增加了私钥及存取密码。

编码格式

PEM - Privacy Enhanced Mail, BASE64编码，可读
Apache和Unix/Linux 服务器采用的编码格式。

2018年8月 (4)
2018年7月 (8)
2018年6月 (2)
2018年5月 (4)
2018年3月 (3)
2018年2月 (5)
2017年10月 (1)
2017年8月 (1)
2017年6月 (1)
2017年3月 (2)
2017年2月 (1)
2017年1月 (4)
2016年12月 (5)
2016年11月 (1)
2016年10月 (4)
2016年9月 (4)
2016年8月 (1)
2016年4月 (1)
2015年12月 (1)
2015年9月 (3)
2015年8月 (1)
2015年7月 (4)
2015年6月 (1)
2015年4月 (3)
2015年3月 (3)
2011年11月 (2)
2011年10月 (2)
2011年9月 (5)

links

ascii 图表
ascii艺术字

最新评论

1. Re:Java条形码生成技术-Barcode4j

DER - Distinguished Encoding Rules,二进制格式,不可读.
Windows 服务器采用的编码格式.

文件扩展名

pem/der 数字证书, 编码格式与其名称对应;
crt 数字证书, 常见于unix/linux系统;
cer 数字证书, 常见于windows系统;
key 非证书, 一般是公钥或私钥文件;
csr certificate signing request, 证书签名请求文件;
pfx/p12 - predecessor of PKCS#12, 是PKCS#12 标准的证书文件,
同时包含了公钥和私钥, 存取时需提供密码, 采用DER 编码

五、样例

获取github 证书

使用chrome 打开 <https://github.com/> ,点击链接左边的 区域可看到信息面板:

找到证书信息, 导出详细信息

证书内容

怎么隐藏条形码下方的文本?或者设置为自定义文本?

--习惯沉淀

2. Re:成为高手前必懂的TCP干货

@
海向

--美码师

3. Re:成为高手前必懂的TCP干货

6

--海向

4. Re:redis通过pipeline提升吞吐量

@ericlfredis-stat , 可参考这里的: ...

--美码师

5. Re:redis通过pipeline提升吞吐量

楼主, 请教下性能测评是使用的什么工具? 3Q!

--ericlf

阅读排行榜

1. 使用 openssl 生成证书(62415)
2. mysql 索引过长1071-max key length is 767 byte(56645)
3. Java条形码生成技术-Barcode4j(36608)
4. MQTT服务器搭建-mosquitto1.4.4安装指南(26266)
5. 使用keytool 生成证书(18705)

评论排行榜

1. 情人节, 送女友一桶代码可否? (36)
2. 软能力那点事, 你知多少(18)
3. 老兵的十年职场之路(一)(9)
4. redis通过pipeline提升吞吐量(6)
5. MQTT服务器搭建-mosquitto1.4.4安装指南(6)



作者: [zale](#)

出处: <http://www.cnblogs.com/littleatp/>, 如果喜欢我的文章, 请关注我的公众号

本文版权归作者和博客园共有, 欢迎转载, 但未经作者同意必须保留此段声明, 且在文章页面明显位置给出 [原文链接](#) 如有问题, 可留言咨询.

分类: [2.安全技术](#)

标签: [SSL/TLS](#)

好文要顶

关注我

收藏该文



[美码师](#)

[关注 - 7](#)

[粉丝 - 90](#)

[+加关注](#)

0

推荐

0

反对

« 上一篇: [使用 openssl 生成证书](#)

» 下一篇: [关于蜂窝物联网技术 NB-IoT 的一些观点](#)

posted @ 2016-09-17 14:33 美码师 阅读(2349) 评论(0) 编辑 收藏

[刷新评论](#) [刷新页面](#) [返回顶部](#)

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

推荐排行榜

1. 软能力那点事, 你知多少(17)
2. 情人节, 送女友一桶代码可否? (15)
3. 老兵的十年职场之路(二)(9)
4. 回顾下自己都写了什么(9)
5. 老兵的十年职场之路(一)(8)

【培训】从Java菜鸟到大牛的成长秘籍 6.18冰点价限时直降1500!

【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：

- [SSL证书生成流程](#)
- [什么是安全证书，访问者到底是怎么校验安全证书的，服务端返回安全证书后，客户端再向谁验证呢？](#)
- [数字证书](#)
- [SSL证书](#)
- [ssl证书验证](#)

最新新闻：

- [鱼在水中也憋气](#)
- [谷歌宣布即将淘汰32位版Android Studio与Android模拟器](#)
- [Mozilla 正式为 Firefox 推出全新 logo](#)
- [天文学家称月球最大的陨石坑下方隐藏着神秘物质](#)
- [可循环利用食品包装透明薄膜问世](#)
- » [更多新闻...](#)

历史上的今天:

2015-09-17 Java条形码生成技术-Barcode4j



Copyright ©2019 美码师