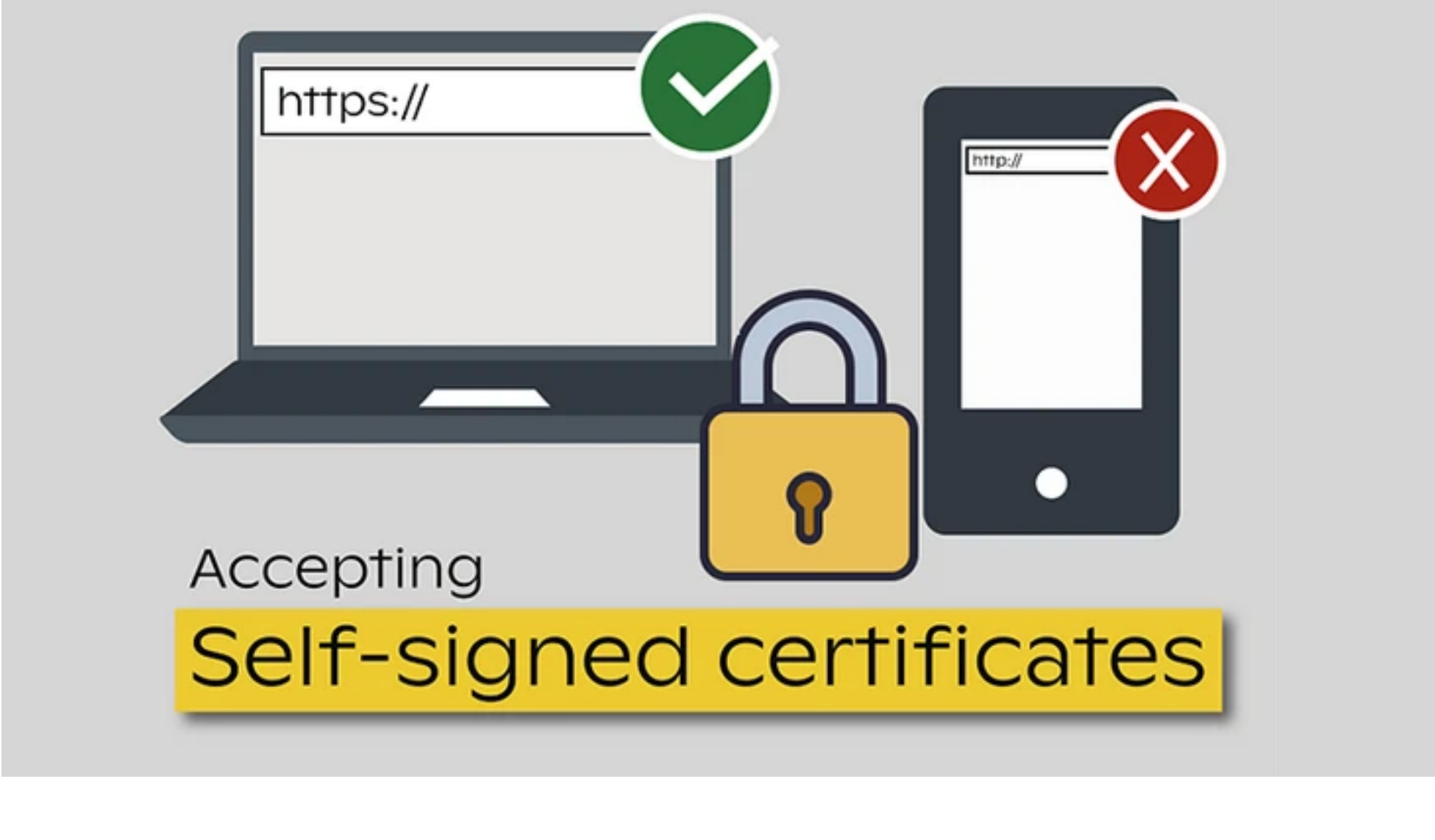


# 什么是自签名证书？自签名SSL证书的优缺点？

 **Anita的大杂烩** 发布于 10 月 19 日

自签名证书可以指许多不同的证书类型，包括**SSL/TLS证书**、**S/MIME证书**、**代码签名证书**等，其中最常见的证书类型是自签名SSL证书。与CA颁发的SSL证书不同，自签名证书通常指的是那些未经第三方验证，直接上传到私有公钥基础结构(PKI)的证书文件。



## 什么是自签名SSL证书？

自签名证书是由不受信的CA机构颁发的数字证书，也就是自己签发的证书。与受信任的CA签发的传统数字证书不同，自签名证书是由一些公司或软件开发商创建、颁发和签名的。虽然自签名证书使用的是与X.509证书相同的加密密钥对架构，但是却缺少受信任第三方（如Sectigo）的验证。在颁发过程中缺乏独立验证会产生额外的风险，这就是为什么对于面向公众的网站和应用程序来说，自签名证书是不安全的。

## 自签名证书有什么优势？

虽然使用自签名证书有风险，但也有其用途。

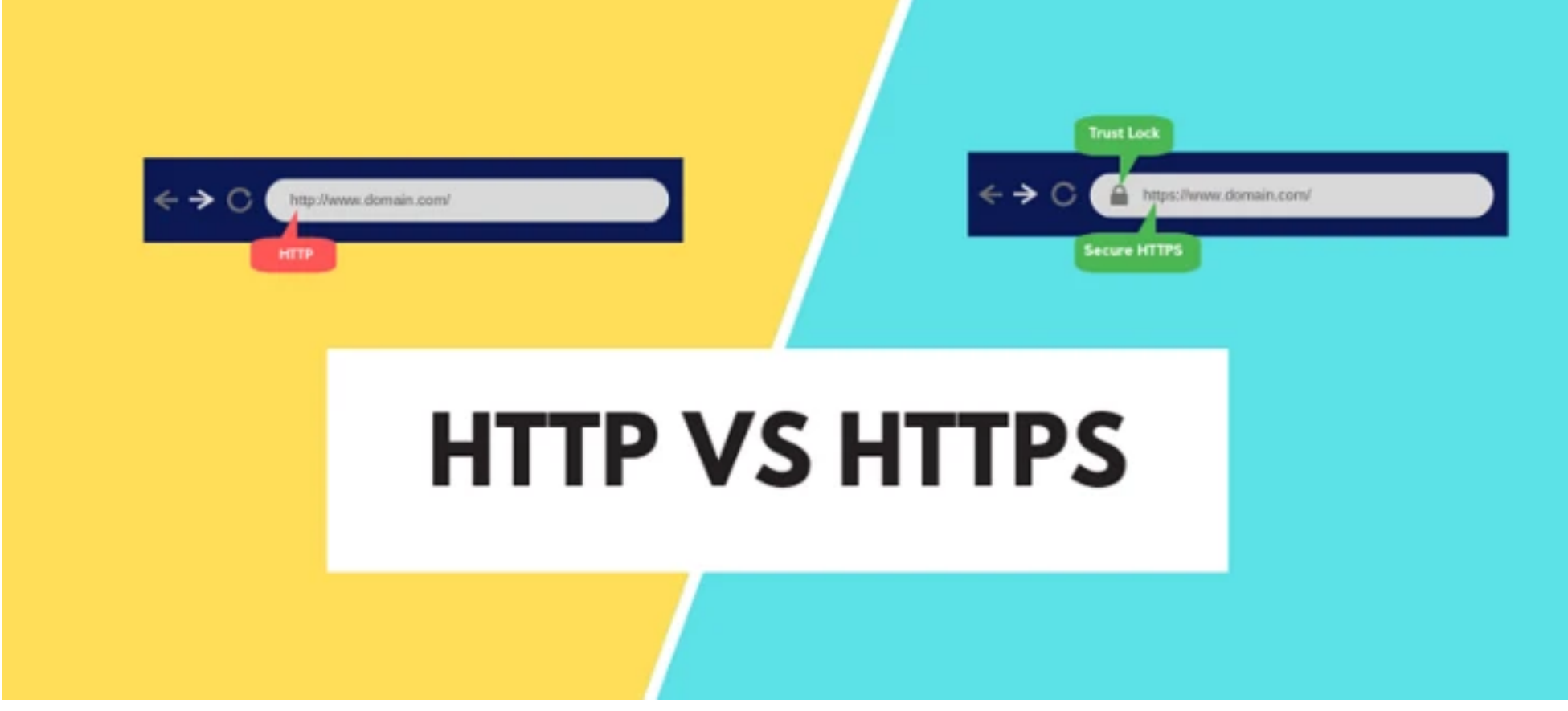
- 免费。自签名证书是免费提供的，任何开发人员都可以申请。
- 随时签发。自签名证书可以随时随地签发，不用等待第三方证书颁发机构的验证和签发。
- 加密。自签名SSL证书使用与其他付费SSL/TLS证书相同的方法加密传输数据。
- 方便。自签名证书不会在一段时间后过期或需要续订，但CA颁发的证书却会在一段时间后过期，还需要续订。

虽然自签名证书看起来很方便，但这也是这些证书的主要问题之一，因为它们无法满足针对发现的漏洞进行安全更新，也不能满足当今现代企业安全所需的证书敏捷性。因此，很少人使用自签名SSL证书。此外，自签名证书无法撤销证书，如果证书被遗忘或保留在恶意行为者开放的系统上，则会暴露所使用的加密方法。不幸的是，即便如此，一些 IT 部门认为，证书颁发机构颁发的证书的成本超过了降低额外验证和漏洞支持的风险。

## 自签名证书有什么缺陷？

### 1、不受浏览器信任，易丢失用户。

每当用户访问使用自签名证书的站点时，他们会收到“不安全”警告，显示诸如“error\_self\_signed\_cert”或“err\_cert\_authority\_invalid”之类的错误，要求用户确认他们愿意承担风险继续浏览。这些警告会给网站访问者带来恐惧和不安，用户会认为该网站已被入侵，无法保护他们的数据，最后选择放弃浏览该站点转而访问不会提示安全警告的竞争对手网站。另外，不受浏览器信任的自签名证书，地址栏不会显示安全锁和HTTPS协议头。下图为SSL证书在浏览器地址栏中的状态显示，左边为自签名SSL证书，右边为受信CA颁发的SSL证书：



### 2、不安全。

由于自签名证书支持超长有效期，因此也无法在发现新的漏洞后进行安全更新，容易受到中间人攻击破解。自签名SSL证书没有可访问的吊销列表，也容易被黑客伪造、假冒网站利用，不能满足当前的安全策略，存在诸多的安全隐患。

## 企业可以使用自签名证书吗？

如前所述，使用自签名证书会带来很多风险，特别是在公共站点上使用自签名证书的风险更大。对于处理任何个人敏感信息的网站，包括健康、税务或财务记录等信息，万万不可使用自签名证书。类似这样的数据泄露会损害用户对品牌的信任度，还会遭到隐私法规的处罚，损害企业的经济利益。

许多人认为在公司内部的员工门户或通信站点部署自签名证书没有风险，但事实并非如此。因为在这些站点使用自签名证书仍会导致浏览器安全警告。虽然可以忽略这些警告，但却无意中助长了员工忽略安全警告的习惯。这种行为习惯可能会使企业今后面临更大的风险。

虽然我们不建议企业使用自签名证书，但它也并不是没有用处。一般来说，自签名证书可以用于内部测试环境或限制外部人员访问的Web服务器。

## 如何创建自签名证书？

虽然自签名证书存在一定的安全隐患，但有它的优势，这里给大家分享一下创建自签名证书的方法。其实，创建自签名SSL证书很简单，主要取决于您的服务器环境，如Apache或Linux服务器。方法如下：

### 1、生成私钥

要创建SSL证书，需要私钥和证书签名请求（CSR）。您可以使用一些生成工具或向CA申请生成私钥，私钥是使用RSA和ECC等算法生成的加密密钥。生成RSA私钥的代码示例：`openssl genrsa -aes256 -out servername.pass.key 4096`，随后该命令会提示您输入密码。

### 2、生成CSR

私钥生成后，您的私钥文件现在将作为 `servername.key` 保存在您的当前目录中，并将用于生成CSR。自签名证书的CSR的代码示例：`openssl req -nodes -new -key servername.key -out servername.csr`。然后需要输入几条信息，包括组织、组织单位、国家、地区、城市和通用名称。通用名称即域名或IP地址。

输入此信息后，`servername.csr` 文件将位于当前目录中，其中包含 `servername.key` 私钥文件。


### 3、颁发证书

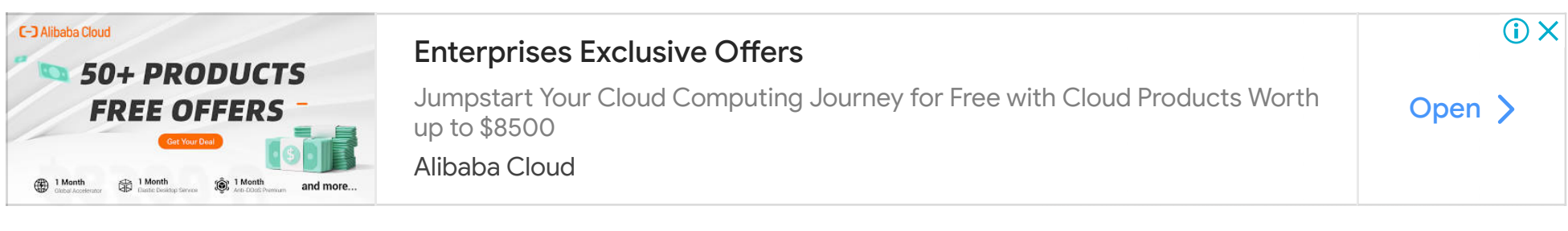
最后，使用`server.key`（私钥文件）和`server.csr` 文件生成新证书（.crt）。以下是生成新证书的命令示例：`openssl x509 -req -sha256 -days 365 -in servername.csr -signkey servername.key -out servername.crt`。最后，在您的当前目录中找到 `servername.crt`文件即可。

创建自签名证书的方法很简单，不需要第三方验证。所以，它是在可以在内部测试环境中使用，但不建议企业在用户环境中使用。企业或组织应该选择受信CA颁发的SSL证书，锐成信息提供**Digicert**、**Sectigo**、**Globalsign**等全球最受信的CA机构颁发的SSL证书，这些证书能帮助您规避用户流失、数据泄露和中间人攻击等安全风险。千万不要为了省小钱而花大钱，要有长远的眼光，才能获得长久的利益！

本文转载于<https://www.racent.com/blog/w...>

ssl证书https安全

 **本文系转载，阅读原文**  
<https://www.racent.com/blog/what-is-a-self-signed-certificate>



阅读 568 · 发布于 10 月 19 日

赞

收藏

分享

 **数字签名**  
网络安全、终端安全知识分享！

关注专栏


 **Anita的大杂烩**  
网络安全、终端安全知识分享！

1 声望 0 粉丝

关注作者

0 条评论

得票数 最新

 撰写评论 ...

提交评论

继续阅读

什么是WHQL微软徽标认证？为什么需要这项认证？

根据微软最新的规定，微软不再接受EV代码签名证书为驱动程序数字签名，而是需要驱动程序开发商申请WHQL认证解决驱动签名的问题。...

Anita的大杂烩 阅读 148

【干货分享】最新WHQL徽标认证申请流程

随着Windows 10版本的发布，微软对WHQL徽标认证的申请流程做了相应的更改。锐成信息将最新WHQL认证申请流程分享出来，方便大家...

Anita的大杂烩 阅读 157

EV代码签名证书有什么特点？靠谱推荐

代码签名证书分为：普通型代码签名证书和增强型代码签名证书，其中增强型代码签名证书也被称为扩展验证代码签名证书，增强型代码签名...

安信证书 阅读 318

网站还在使用自签名SSL证书？大错特错

自签名SSL证书是什么？估计很多人还不了解，但也有不少人在使用。至于使用的情况如何，我猜是如人饮水冷暖自知。要想对它有个全面的...

安信证书 阅读 209

开发者为什么需要EV代码签名证书

代码签名证书是数字证书的其中一种，该证书能够对代码进行有效“签名”，能够识别软件由来是否安全以及软件开发者的真实身份是否有效...

安信证书 阅读 244

安装Sectigo代码签名证书的好处及申请价格

Sectigo是世界知名的SSL数字证书颁发机构，拥有二十多年的历史，在150多个国家或地区中拥有超过1亿张数字证书。其SSL证书类型丰富...

安信证书 阅读 513

什么是SSL证书链？

证书包含的内容可以概述为三部分，用户的信息、用户的公钥、还有CA中心对该证书里面的信息的签名。我们在验证证书的有效性的时候，...

沃通CA 阅读 529

靠谱的SSL证书颁发机构推荐

相信很多人都知道了SSL证书的重要性，SSL证书主要有数据加密传输和证明网站真实身份的作用。而近年来数据泄露事件频发，更突显了它...

安信证书 阅读 267