

## HTTPS 证书颁发机构 Startssl SSL 申请图文详解

### 一、什么是 SSL 证书，什么是 HTTPS 网站？

SSL 证书是数字证书的一种，类似于驾驶证、护照和营业执照的电子副本。SSL 证书通过在客户端浏览器和 Web 服务器之间建立一条 SSL 安全通道(Secure socket layer(SSL)安全协议是由 Netscape Communication 公司设计开发。该安全协议主要用来提供对用户和服务器的认证;对传送的数据进行加密和隐藏;确保数据在传送中不被改变，即数据的完整性，现已成为该领域中全球化的标准。由于 SSL 技术已建立到所有主要的浏览器和 WEB 服务器程序中，因此，仅需安装服务器证书就可以激活该功能了)。即通过它可以激活 SSL 协议，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露。保证了双方传递信息的安全性，而且用户可以通过服务器证书验证他所访问的网站是否是真实可靠。

### 二、什么网站需要 SSL 证书？

就我遇到过的网站，配置了认证的证书的，大概有这么几类：

#### 1、购物交易类网站

这个就不用说了，支付宝、Paypal 等肯定会加密以保护你的密码安全。

#### 2、注册类站点

有些大站点，注册会员或者登陆的时候，会专门通过 SSL 通道，来保护你的密码安全，比如：

<https://www.name.com/account/login.php>

<https://idp.godaddy.com/login.aspx>

### 三、Startssl SSL 申请详细步骤(<http://www.startssl.com/?app=21>)

1，先要在 Startssl 上注册用户，注册界面如下，注册后需要等待审核通过。

**Important: Read and follow all instructions carefully! You are required to adhere to our terms and conditions!**

First, Last Name:   ?

Complete Home Address (Street, House, Number):  ? 地址要写详细, 要精确到门牌号。

Zip, Locality/Place:  ,  Beijing ?

Country:  China v

State/Region \*\*:  v

Phone:  +86 ?

Email \*:  ? 不要用qq等后缀邮箱, 最好用Gmail邮箱

Clear

Continue >>>

\* Mail accounts from the following providers are not allowed: qq.com freemail.com rambler.ru mailnull.com laposte.fr yopmail.com

\*\* Not seeing the States/Regions? Make sure you have JavaScript enabled.

深度VPS deepvps.com

\*\* States/Regions still missing of your country? Please help to improve it! Send a complete list to us.



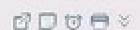
2、如果审核通过, 你会在你注册的时候的邮箱内收到一封内容类似于下面的邮件, 你按链接点过去, 照提示一步一步就可以在你浏览器上安装一个证书了, 这个证书用来做 Startssl 认证的, Startssl 只提供证书认证, 所以如果你丢了证书, 那只能重新注册用户了。

**StartSSL Account Request, 24 Oct 2010 08:54 ☆**

发件人: **StartCom CertMaster (Sapir Kahlon)** <certmaster@startcom.org> 查看 拒收

时 间: 2010年10月24日(星期天) 下午2:54

收件人: iamfly2004 <iamfly2004@gmail.com>



To Liu Chen,

Your request for an account at StartSSL (www.startssl.com) has been approved and is available during the next 24 hours at the following location:

[https://www.startssl.com/?app=12&action=release&id=\[REDACTED\]&auth=\[REDACTED\]](https://www.startssl.com/?app=12&action=release&id=[REDACTED]&auth=[REDACTED])

The verification code in order to continue the process is [REDACTED]

点这个链接过去激活账户, 然后按照提示安装证书。最好用Firefox安装, IE可能会安装不上。

Thank you!

StartCom Ltd.

StartSSL Certification Authority


深度VPS deepvps.com

3、当认证通过后，就可以看到下面的界面了，我们先做验证向导，这里需要我们有自己的域名，且有域名注册时的邮箱，这步的作用就是验证你是否是域名的拥有者，相应步骤如下。

Tool Box

Certificates Wizard

Validations Wizard



Select Validation

- Select the type and attribute of validation you'd like to perform.
- Please note that you might need to have instant access to your email account(s) or documents in image format ready.

Type:


Continue >>>

深度VPS [deepvps.com](http://deepvps.com)

Tool Box

Certificates Wizard

Validations Wizard




Enter Domain Name

- Enter the domain name you want to have validated.
- You must be the owner of the top-level domain, sub domains are not supported.

http://  .

Continue >>>

深度VPS [deepvps.com](http://deepvps.com)

Tool Box	Certificates Wizard	Validations Wizard	
----------	---------------------	--------------------	---

### Select Verification Email

- Select the email address for verification of domain ownership from below.

**Verification Email:**

☐ postmaster@300host.com

☐ hostmaster@300host.com

☐ webmaster@300host.com

☒ iamfly2020@yahoo.cn **确认域名所有者邮箱，会往这个邮箱里面发一个域名确认码**

☐ domain.tech@yahoo-inc.com

**Continue >>>**

深度VPS [deepvps.com](http://deepvps.com)

#### Your Authentication Code, 24 Oct 2010 03:43

 StartCom CertMaster <certmaster@startcom.org> [新增联系人] [拒收] [举报垃圾邮件] [邮件头] [邮件原文] [打开新窗口]  
收件人: webmaster@300host.com

This mail is intended for the person who requested verification of domain control at StartSSL™ (<http://www.startssl.com>).


Your verification code is **[REDACTED]**

Copy and paste this code now into the form at your open browser window.

Thank you!

StartCom Ltd.  
StartSSL™ Certification Authority

深度VPS [deepvps.com](http://deepvps.com)

Tool Box	Certificates Wizard	Validations Wizard	
----------	---------------------	--------------------	---

### Complete Validation

- A verification code has been sent to "webmaster@300host.com".
- Please check your email account now and enter the code into the text field below.

**Verification Code:**

**Continue >>>**

深度VPS [deepvps.com](http://deepvps.com)

Tool Box

Certificates Wizard

Validations Wizard



**Validation Success**

- You have successfully authenticated domain "300host.com".
- You will be able to use this verification for the next 30 days, after which it expires and must be renewed.

Finish >>>

深度VPS [deepvps.com](http://deepvps.com)

4、下面再做 https 证书申请向导，相应步骤如下。记得一定要按提示保存好那个私钥文件，否则到后面证书文件得到了，私钥文件丢了，就没法在做认证了。

Tool Box

Certificates Wizard

Validations Wizard



**Select Certificate Purpose**

- Make sure you have already validated a domain name or email address before using this tool! Select the "Validations Wizard" for this task.
- Depending on your preferences and type of software, you need to have a prepared certificate request (CSR) ready for submission.

Certificate Target: Web Server SSL/TLS Certificate

Continue >>>


深度VPS [deepvps.com](http://deepvps.com)



Tool Box

Certificates Wizard

Validations Wizard



### Generate Private Key

- If you created your own private key and certificate request (CSR), **please skip this step.**
- Provide a password for your private key. (At least 10 characters, max. 32)
- Allowed are only letters and numbers, without spaces!
- Please remember it or write it down somewhere...

这里也可以点 skip，但那需要你在 VPS 上用 openssl 已经生成好了私钥和证书申请文件

Key Password:

Confirm Password:

Keysize:

2048 (Medium)

Skip >>>

Continue >>>

深度VPS [deepvps.com](http://deepvps.com)

Tool Box

Certificates Wizard

Validations Wizard



### Save Private Key

- Copy and paste the content from the textbox below into a file and save it as **ssl.key**.
- Make sure, that you do not alter the content and you did not add any spaces! Save it in ASCII format (plain text).
- Allowed are only letters and numbers, without spaces!
- Decrypt the private key with the OpenSSL utility: **openssl rsa -in ssl.key -out ssl.key** or use the utility from the Tool Box.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,ED061B1D82C03D40C485BA30237E2D38

EwhOQvPolGjaZvui9HFKOwhT628ImbcEmghw1iDRSD6nwKolo5FUTgJtzq6cyNFV
56KXGxeQ1vb1arVibPKD6+aG53LNi2BclkFGryQnSb1miyOnhMcUi46CU48r97Tf
rVuu7kzuS+cv35a0lidEul.3vXexnOUJOcGF6OfnWFwhkixSNnWGMvSk7nDUi58VX
```

保存这段代码为 ssl.key，这个就是私钥文件

Continue >>>

深度VPS [deepvps.com](http://deepvps.com)

Tool Box	Certificates Wizard	Validations Wizard	
----------	---------------------	--------------------	---

### Add Domains

- Select the top target domain name for your certificate.
- Note: Only domain names which were validated within the last 30 days are eligible for selection.

Domain:  

[Continue >>>](#)

[深度VPS deepvps.com](#)


Tool Box	Certificates Wizard	Validations Wizard	
----------	---------------------	--------------------	---

### Ready Processing Certificate

- We have gathered enough information in order to sign your certificate now.
- The common name of this certificate will be set to **ssl.300host.com**.
- The certificate will have the following host names supported:
  1. **300host.com**
  2. **ssl.300host.com**
- Please click on *Continue* in order to process the certificate.

[Continue >>>](#)

[深度VPS deepvps.com](#)

Tool Box	Certificates Wizard	Validations Wizard	
----------	---------------------	--------------------	---

### Additional Check Required!

 You successfully finished the process for your certificate. However your certificate request has been marked for approval by our personnel. Please wait for a mail notification from us within the next 3 hours (the most). We might contact you for further questions or issue the certificate within that time. Thank you for your understanding!

[深度VPS deepvps.com](#)

**StartSSL Certificate issued, 25 Oct 2010 02:41**

 StartCom CertMaster (Nikolay Duhman) <certmaster@startcom.org> [新增联系人] [拒收] [举报垃圾邮件] [邮件头] [邮件原文] [打开新窗口]

收件人: webmaster@300host.com

To Liu Chen,

This mail concerns the digital certificate you requested from the StartCom Certification Authority (<http://www.startssl.com>). Your certificate with serial number 151243  
<https://www.startssl.com/?app=12>

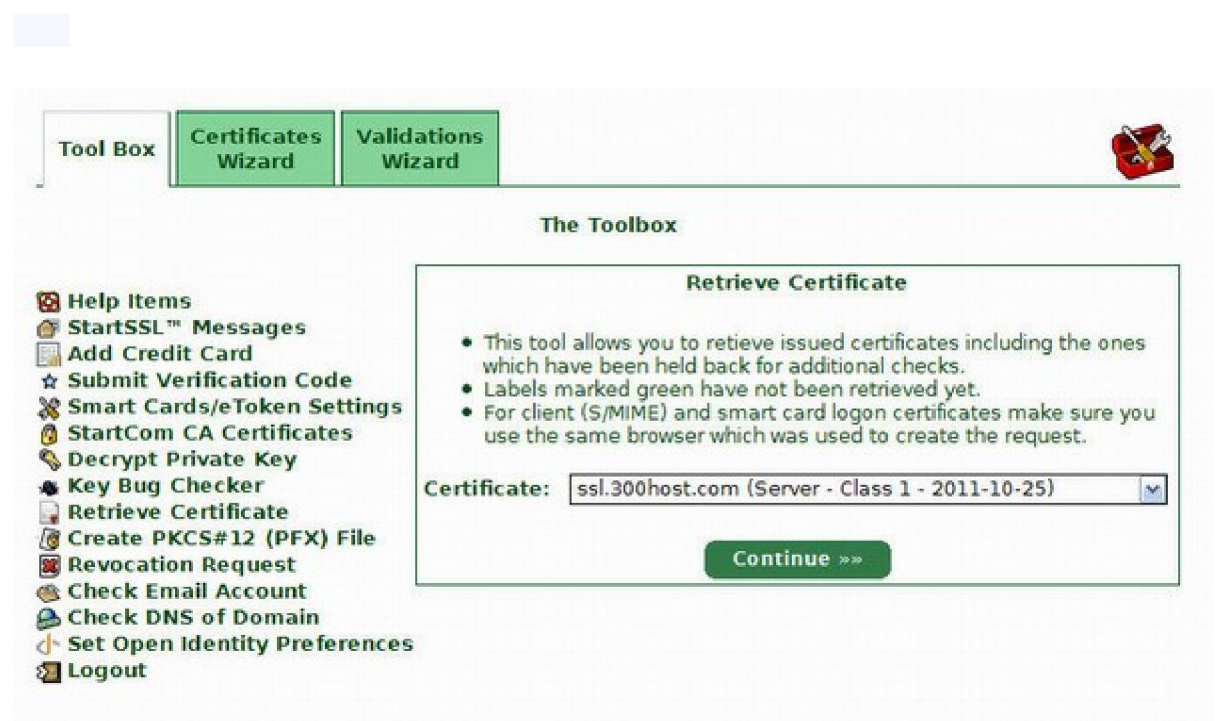
Please login to your account and select from the Tool Box tab the section Retrieve Certificate. The pending certificate is marked with a green colored label.


Thank you!

当你收到这个邮件后，再去 [startssl.com](http://www.startssl.com) 中的 tool box 下的 retrieve certificate 中，就可以下载到你申请域名的证书文件啦

深度VPS [deepvps.com](http://deepvps.com)

5、下面就等待几个小时，去邮箱看看刚申请的域名 https 证书是否成功得到了，如果得到了，就去下载证书文件就是了，相应步骤如下。




**Tool Box** Certificates Wizard Validations Wizard 

**The Toolbox**

**Retrieve Certificate**

- This tool allows you to retrieve issued certificates including the ones which have been held back for additional checks.
- Labels marked green have not been retrieved yet.
- For client (S/MIME) and smart card logon certificates make sure you use the same browser which was used to create the request.

Certificate:  

**Continue** >>>

**Help Items**

- StartSSL™ Messages
- Add Credit Card
- Submit Verification Code
- Smart Cards/eToken Settings
- StartCom CA Certificates
- Decrypt Private Key
- Key Bug Checker
- Retrieve Certificate
- Create PKCS#12 (PFX) File
- Revocation Request
- Check Email Account
- Check DNS of Domain
- Set Open Identity Preferences
- Logout





最后，Startssl SSL 证书就算申请好了，下一篇给大家介绍一下怎样在 Nginx 环境下面配置 SSL 证书，敬请期待。