# HTTPS Certificate Creation Manual

Version: 0.0.0
Release date: February 7, 2014

**Specifications are subject to change without notice.**

**Liability Disclaimer**

Fanvil may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked as reserved or undefined. Fanvil reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Fanvil sales office or your distributor to obtain the latest specification and before placing your product order.

# Table of Contents

# 1 Revision History

**Revision history:**

| Revision | Author | Date | Description |
|---|---|---|---|
| 0.0.0 | Song Jupo | February 7, 2014 | Initial version |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 2 Introduction

## 2.1 Overview

HTTPS is a secure transport protocol with ssl encryption, which supports data encrtyption and authentication, so it is more secure than HTTP Protocol. The protocol can establish a secure channel of information, all data submitted will be encrypted before submission, thus to ensure the security of data transmission.
Before using phone Web's HTTPS, you need to install HTTPS certificate.

Phone models that support HTTPS:

- C58/C60/C62/F66
- E01/E52/E58/ E62/E66
- F01/F52/F58/ F62/F66

## 2.2 Target Audience

This document's target audience are internal staffs and customers that want to use Web HTTPS.

# 3 OpenVPN Server's Download And Installation

Search and download the Windows version of the OpenVPN software on the Internet.
Double click the downloaded software, and intall it with default settings, the default install path is C:\Program Files\OpenVPN.

# 4 Server Configuration

## 4.1 Initiation

Before using HTTPS, we should do some initialization work.
Open document C:\Program Files\OPENVPN\easy-rsa\vars.bat.sample, the following part need to be modified.

```
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=FortFunston
set KEY_EMAIL=mail@domain.com
```

(Please change settings according to your own situation):

```
set HOME=C:\Program Files\OPENVPN\easy-rsa
set KEY_COUNTRY=CN                          #(Country)
set KEY_PROVINCE=BEIJING                    #(Province)
set KEY_CITY=BEIJING                        #(City)
set KEY_ORG=WINLINE                         #(Orgnization)
set KEY_EMAIL=admin@winline.com.cn          #(Email)
```

Everything after # are comments, please don't write file.

Then enter the command line (Start > Run - > CMD into DOS):
Enter dirctory of openvpn\easy-rsa.
Execute follow commands:

**init-config**
**vars**
**clean-all**

Note: The above is the initialization work, after the initialization, when you want to create certificate, you still need to initialize, but only need to enter the openvpn\easy-rsa directory, and run vars only, do not need run all of those steps. (If your server has been built, then make HTTPS certificate from this step).

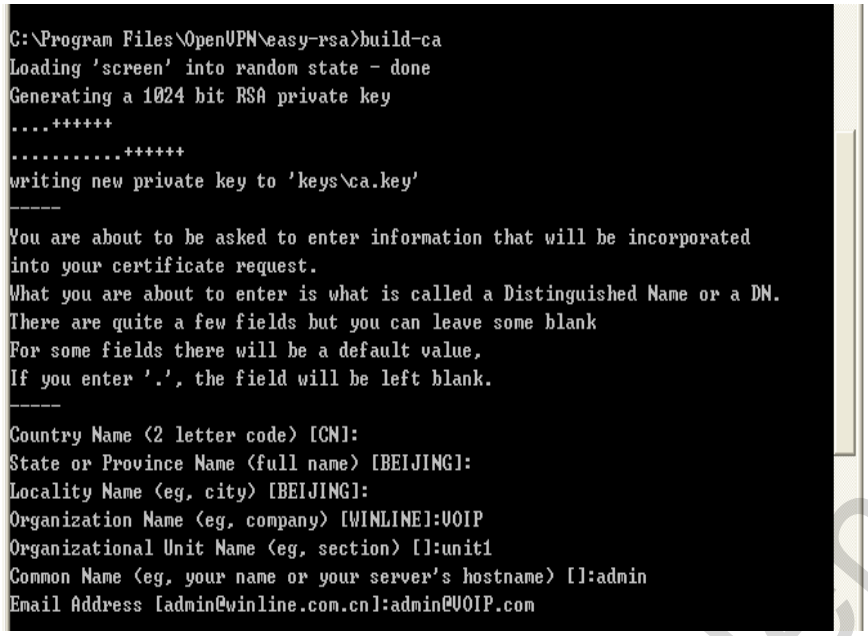
## 4.2 Certificate Creation

**Generate the root CA:**

Input command "**build-ca**" and press Enter key.

```
Country Name (2 letter code) [CN]:)                                  # (Can not fill)
State or Province Name (full name) [BEIJING]:                        # (Can not fill)
Locality Name (eg, city) [BEIJING]:                                  # (Can not fill)
Organization Name (eg, company) [WINLINE]:                           # (Fill your own info)
Organizational Unit Name (eg, section) []:unit1                      # (Fill your own info)
Common Name (eg, your name or your server's hostname) []:admin       # (Fill your own info)
Email Address [admin@winline.com.cn]:          #( Common Name@ Organization Name.com)
```

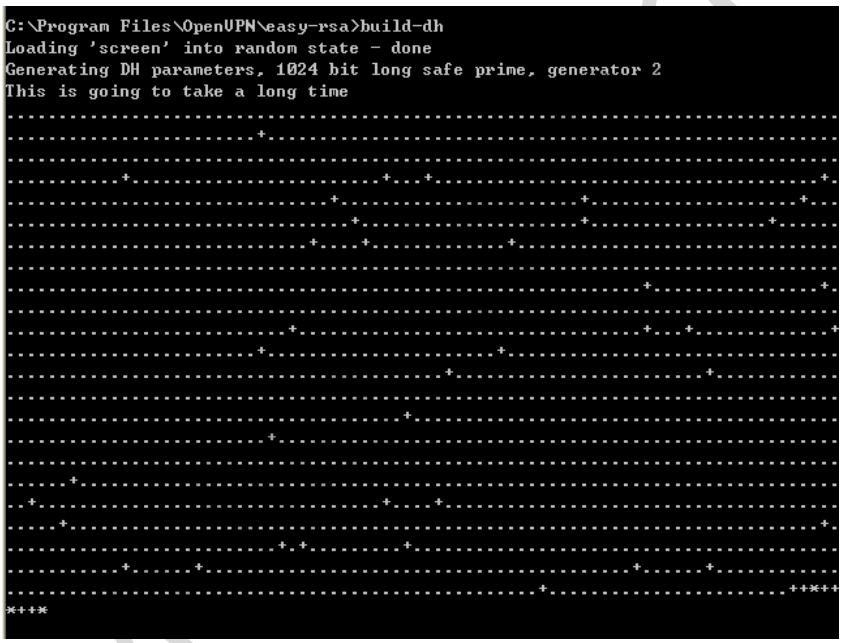
As shown in Figure：




Input command "**build-dh**" and press Enter key.

This step requires a longer time, please wait patiently.

As shown in Figure：




**Generate Server Key:**

Enter "**build-key-server server**", press the Enter key (The command "build-key-server" is fixed, can not be changed; the "server" can be changed, but in order for facilitate, we advice to use server related words).

After that, it will prompt you to enter the following information:

Country Name (2 letter code) [CN]: # (Consistent with the root CA)

State or Province Name (full name) [BEIJING]: # (Consistent with the root CA)

Locality Name (eg, city) [BEIJING]: # (Can be different)

Organization Name (eg, company) [WINLINE]: # (Consistent with the root CA)
Organizational Unit Name (eg, section) []:unit1 # (Fill your own info)
Common Name (eg, your name or your server's hostname) []: adminServer # (Fill your own info)
Email Address [admin@winline.com.cn]: # (Can be different)
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:adminServer #(Fill your own info)
An optional company name []:winline #(Fill your own info)
Certificate is to be certified until Nov 24 06:24:34 2018 GMT (3650 days)
Sign the certificate? [y/n]:y #(Select 'y')
1 out of 1 certificate requests certified, commit? [y/n]y #(Select 'y')
The generated key stored in the openvpn\easy-rsa\keys directory.
As shown in Figure:

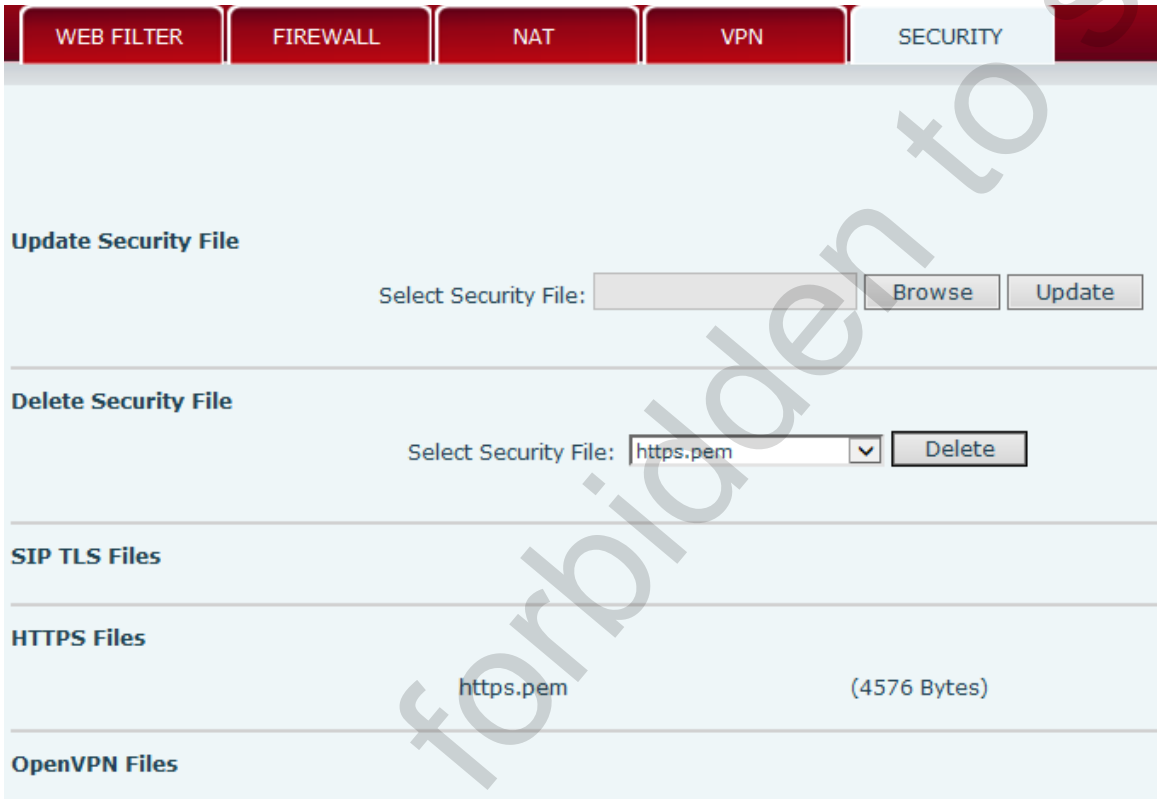
# 5 Generate HTTPS Certificate

Find server.key, server.crt files in the openvpn\easy-rsa\keys directory, then append server.key's content to the server.crt, after that you should rename server.crt to https.pem, https.pem is the HTTPS's certificate that we will use.
So far, HTTPS certificate is created.

# 6 Use HTTPS Certificate

## 6.1 Upgrade HTTPS Certificate

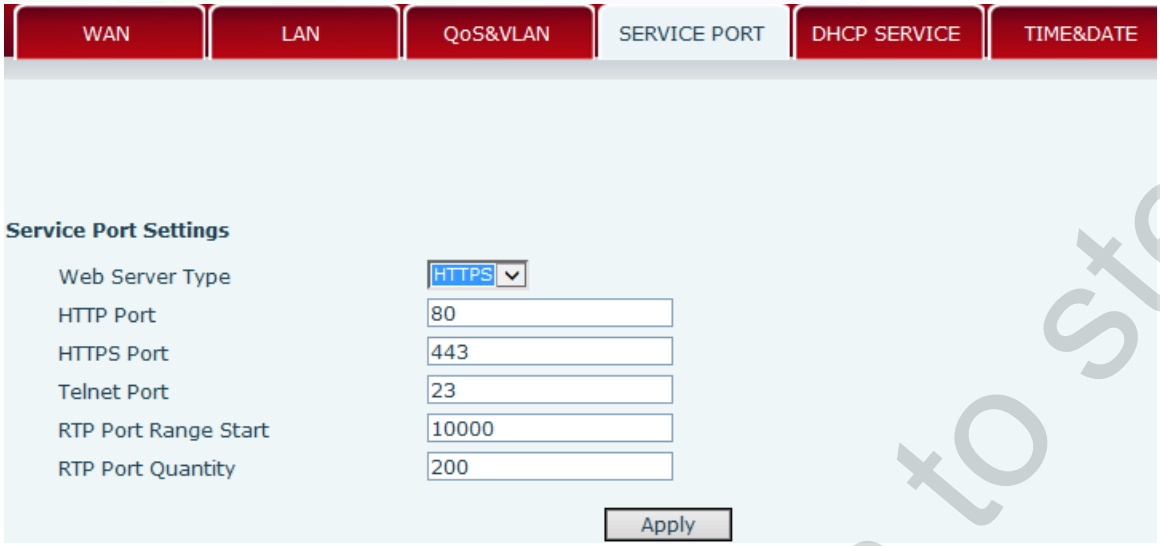
Logon the phone's Web, find SECUTITY-SECURITY-Update Security File page, then click the Browse button and select the https.pem, click the Update button to upgrade.
As shown in Figure:




After the upgrade is complete, Delete Security File drop-down box and HTTPS FILES will show upgraded certificate file.

## 6.2 Set HTTPS Web Type

Find Webpage NETWORK-SERVICE PORT, then select Web Server Type to HTTPS and modify the HTTPS Port's value; After setting click the Apply button to submit andrestart the phone.
As shown in Figure:




If the phone is not restart, it will still use the original Web Server Type; HTTPS Web Server Type will take effect after phone restart.

## 6.3 Logon HTTPS Web Server

After the restart, the phone can use the new URL to logon. The new URL is https://Phone IP:HTTPS Port.