linkingvision

Domain-based HTTPS certificate

White paper

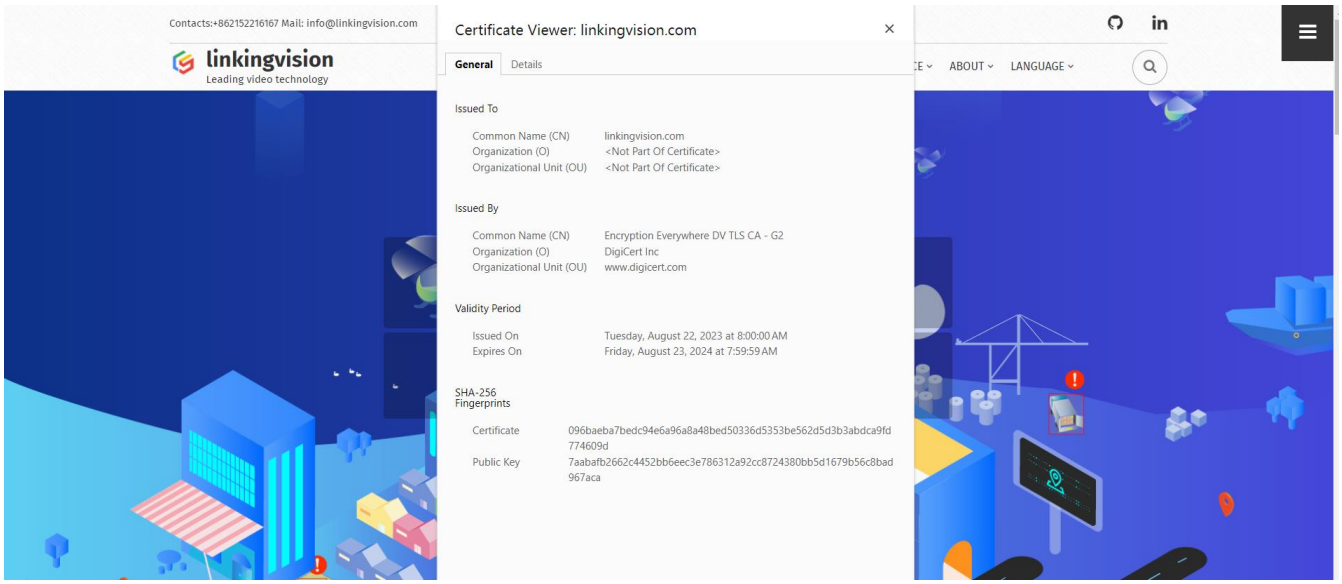
Version records

Version	Date	Describe

Content

1.0 Background Introduction

If you want to make the browser trust a HTTPS service (hereinafter referred to as the service), the service must use a certificate that is on the browser's trusted certificate chain. Generally, certificates need to be purchased and bound to a domain name, similar to the following image:



2.0 Configuration method

2.1 Server configuration

First, purchase an https certificate online. It is recommended to purchase an https certificate on Alibaba. After purchasing the certificate, download the type of certificate file. It is recommended to download the nginx type of certificate file. After decompressing the downloaded certificate file, you will get two files with the key and pem suffixes. (This example uses Linux, but the certificate file for Windows is also a compressed file.) As shown in the following figure:

```
-rw-r--r-- 1 root root 1675 May 28  2019 2275836_linkingvision.cn.key
-rw-r--r-- 1 root root 4073 May 28  2019 2275836_linkingvision.cn_nginx.zip
-rw-r--r-- 1 root root 3683 May 28  2019 2275836_linkingvision.cn.pem
```

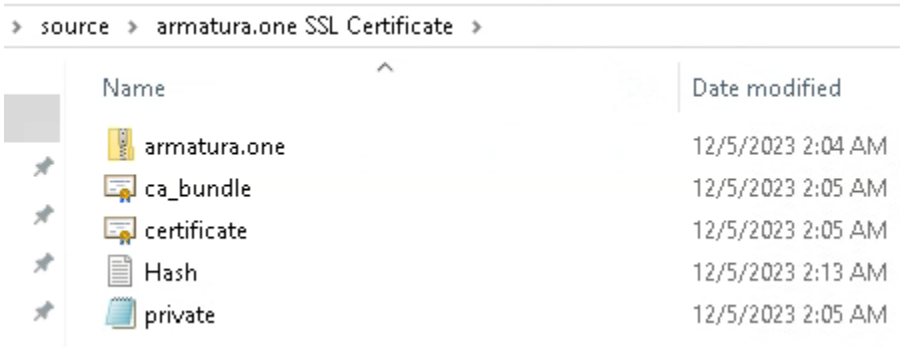
If you are using an nginx type certificate, you can refer to the h5s user manual for the https certificate configuration section.

Use a text compiler (note pad++is recommended) to first clear the content in server.pem, and copy the PEM file and key file contents of nginx to server.pem one after another. The final file structure can refer to the following figure.

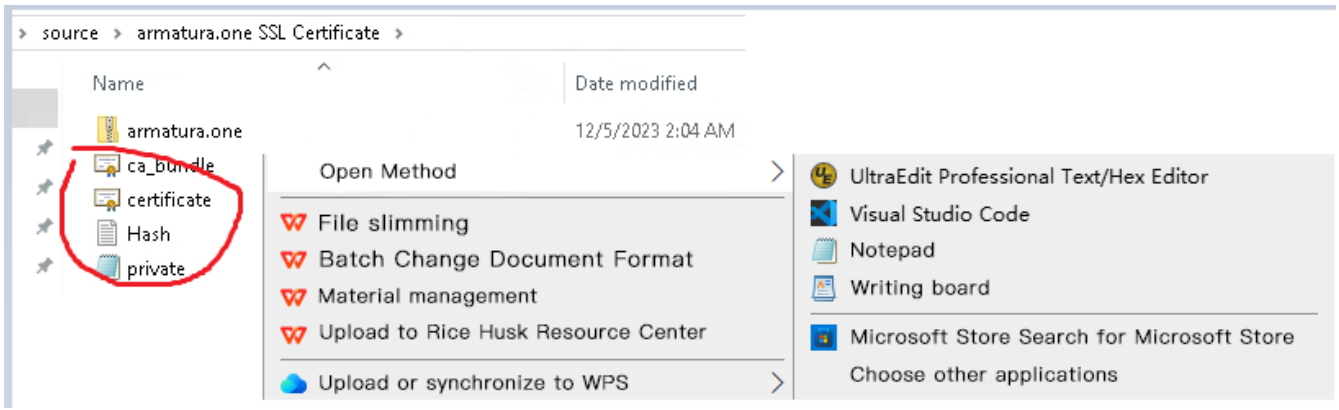
After modifying the server.pem file, restart the H5S service.

```
-----BEGIN CERTIFICATE-----
MIIFmjCCBIKgAwIBAgIQAxUnQ0MmWu5Wvp2tJGP97DANBgkqhkiG9w0BAQsFADBu
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS0wKwYDVQQDEyRFbmNyeXB0aW9uIEV2ZXJ5d2hlcmUg
RFYgVExTIENBIC0gRzEwHhcNMTkwNTI4MDAwMDAwWhcNMjAwNTI3MTIwMDAwWjAb
7Mc31qu89bgElDANBgkqhkiG9w0BAQsFAAOCAQEASocB2iatuVqWiSaWYFSJD5tg
HMbD0VYOfP5+PuMMgjA5O6bhPNLA2x3l5sz6006TvyWoLMzBo2vhRYpow8NxPuw/
EWog5KsH7cD1DquXnRa0X5ATcAxusvrS2egG5i9dOANydpyzUulB3+Xzjsn5RMqa
ra6G0F6GuCG2FvEJTjCriXz/RJcwIWXoY7etXoBQaHuNGqKXS5caz1JhZSQ2ZCuG
wH8AdYZV46Gj6/gRk1G+r6nH3nv6jMUUfL046Geh5NPGMk1QLZinzsaImYKUjWDa
2RgexB7MAsSEduCCSRqfptQQ3Or7cPxOcRgnDrMmqm2ReiM2Ng8kpCZJgNRlpg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgIQAnmsRYvBskWr+YBTzSybsTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xNzExMjcxMjQ2MTBaFw0yNzExMjcxMjQ2MTBaMG4xCzAJBgNVBAYTAlVT
SwW3AU4ETK+GQf2kFzYZkby5SFrHdPomunx2HBzViUchGoofGgg7gHW0W3MlQAXW
M0r5LUvStcr82QDWYNPaUy4taCQmyaJ+VB+6wxHstSigOlSNF2a6vg4rgexixeiV
4YSB03Yqp2t3TeZHM9ESfkus74nQyW7pRGezj+TC44xCagCQQOzzNmzEAP2SnCrJ
sNE2DpRVMnL8J6xBRdjmOsC3N6cQuKuRXbzByVBjCqAA8t1L0I+9wXJerLPyErjy
rMKWaBFLmfK/AHNF4ZihwPGOc7w6UHczBZXH5RFzJNnww+WnKuTPI0HfnVH8lg==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAhaIiLhCi4Z0tSx9CZ+tIlxXtTCsLTIUnuYFuIwDPlS0aUUTB
IlX26XjfyjMwkQUeanGuGUC+CKW4akouTod8E04vcrAqXoLBwqnx0XMV2LiV4Cax
5b8GdLlf62xajR/M6G07LqSIqi08PTyJPTXVIRYbDqvxO8hUIhMnUUaL5iIMP0N8
Pm+JhDiJAqiDmpimsGSkqGbvuytRCBVEmIRVloFjkFYwLtBrqiA8cMo+alkRGquJ
Dha+eP5yhqTl3QuaFgcs/QNU5WpvF+4KX9XrhrYvvXW2jkRNO2fCrspbN4hQx8p5
2P4zrwKBgDuFkBgU5HyO5C6qyFbNuA62lIe9p/kE/PeN2BriIQaT0ShQt3ZWAL/n
xqWnU8J1JM4jhW7ngopGCPXn3FZk2hHoPtYF4sRlOGhXASGAE6BAv+POxsbu8WNk
i2AIw1Q/6BOza0WoPr/rqz0XCOs2A0+FTqoxpeM4wPuzOnlxtKAp
-----END RSA PRIVATE KEY-----
```

There is another situation where the https certificate is not purchased on Alibaba, but on other platforms or locations. The certificate type after purchase is not nginx, but in other formats. After decompression, there are no files with the pem or key suffixes, as shown in the following image:



Then right-click to edit each file after unzipping (it is recommended to use the notepad++ text compiler, including the following copying operation, also using notepad++). Don't worry about the file icon, just right-click to edit each file and view the contents inside each file.



Until the file content can be matched with the server.pem file field of h5s. Then copy the corresponding file content to the server.pem file of h5s in order (clear the contents of the server.pem file before copying). The file format cannot be messed up when copying, as shown in the following figure:


server.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIEODCCAiCgAwIBAgIJALLafhvTZqPDMA0GCSqGSIb3DQEBCwUAMFAxCzAJBgNV
BAYTAkNOMREwDwYDVQQIDAhTaGFuZ2hhaTEWMBQGA1UECgwNbGlua2luZ3Zpc2v
bjEWMBQGA1UEAwwNbGlua2luZ3Zpc2lvbjAeFw0yMjA3MDQwOTE0MzBaFw0zMjA3
MDEwOTE0MzBaMFIxCzAJBgNVBAYTAkNOMREwDwYDVQQIDAhTaGFuZ2hhaTEWMBQG
A1UECgwNbGlua2luZ3Zpc2lvbjEYMBYGA1UEAwwPMTkyLjE2OC4xMDAuMTQ1MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4ycKp84AT5uJcvhhOdebXpEc
MOYp9ALK2SLDGTkdFdRtNhS5/ZcuQGD0CS/+Kuxe5pjbhQyhCf2rquPrjkzIDgyv
uj+X83MN4WdEdCQWYjN5sd3RsuWUxZGnNTCnkD+r+peTKiZOrPHCxoLCOhLcfzcD
AsaIg6WG02cM1DfowaWCv2N/cIgP26KfCJTXQk4TXGqoFrRS9fTOONZuxy50xErd
RiMhhkk18H6wHSG4IwQ8loM3HjR3AEC/8uSIxQUGXhfHGem/rESqcaY1iDhN3+vz
ucDnJHsF4lJwvCJ0kQ4GzoRQjT+CCvRH3z1I635Dnu67MAMKGgDJkw4UNjjLUQID
AQABoxMwETAPBgNVHREECDAGhwTAqGSRMA0GCSqGSIb3DQEBCwUAA4ICAQBEpEXg
mgWokhuq4sY5hWE/tzSrA1ozQ45VY3b47cvyupJRC3Q3LudMOox5INyoa7Gff2hk
ZP1z3zqPWZL8aWyPa3NLu9k0UFb2HC8KfifRUBUy3YJhfvL2qs4lWsnxRTFyu3i5
zETClbNdqTkSIdmrIfersq39TbqlUsMM7xTM6gfUhkNl3nEqOc366lm5y5ybJnt9
UGief8/sHGcErYRmhLYF0uZwooPgMncvTR6jeISlaRJY0Kj3di1tHzymXOvXYm31
W3mDOo5gu2gwCGHcYwKnhKo0eO9YxZ68ZnRRVwfRvr4cswoJbr+ZnXsTLPwTwk1Y
uz7frgA0Cf78a975erbw8+qPSmamtbwuI2OtaOqIZF9Xg09WsmuHZXg45Vs4iRTP
+J+mUirZGSGD26BmQTUimvZPF1R04SiZQb8WUw/ufRZMcJXnXkrB1mIWVpgabnTM
p269UPf//qfawtL6hgIqLDF4dS9hxtryvk2b51iZSUW6kup/eovVbNOxjL2EvUC0
TRBdwyaoGfVW2FL9RccqiMQBAcdgunGrVXnE9s4yPDKW7qp8S/nTuoAeMklSCby2
ovP+CCZw3YRtpXJwh6ZMJqv42wz5/WgMs9MOIpQhBlDz6wVD5b4TP1/Qo5aNcpSL
sTuDExuD5cigEkzo58uf7LsGKmmERxVLeP8WCw==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA4ycKp84AT5uJcvhhOdebXpEcMOYp9ALK2SLDGTkdFdRtNhS5
/ZcuQGD0CS/+Kuxe5pjbhQyhCf2rquPrjkzIDgyvuj+X83MN4WdEdCQWYjN5sd3R
suWUxZGnNTCnkD+r+peTKiZOrPHCxoLCOhLcfzcDAsaIg6WG02cM1DfowaWCv2N/
cIgP26KfCJTXQk4TXGqoFrRS9fTOONZuxy50xErdRiMhhkk18H6wHSG4IwQ8loM3
HjR3AEC/8uSIxQUGXhfHGem/rESqcaY1iDhN3+vzucDnJHsF4lJwvCJ0kQ4GzoRQ
jT+CCvRH3z1I635Dnu67MAMKGgDJkw4UNjjLUQIDAQABAoIBAQCLVmKR5qqIKqeY
r8WsHpa+3pKFaFppxOC7azh0G3W8805+sx4X8Ym8kfyAOkFWASKBn1hg+As8vq90
J1VSN8Ur4RpWTDYgbv4fuyHhgFV+rYbD1YaRj4S/4IXJ+et/b59GG355h4ARVEef
T4xm5TT+kDc3l6Mb5gibWwYik50iUwWUiOPTIl1SFLm650yrsAnUs0IRQF/pvmnn
9VVfFaHeC4iDt+pxhXIvstUKFlh9zVumLXSD5QtT+g2YTuLZxe7e7sj0GsHwAw5Y
JqvvZx5MGV3KcMvB2nMJxot+mBE75fBw6icyb6UWwYw6OcjeMnBO8MFR0X1cggi
VG3ek+aFAoGBAPtVKTq+PKm6/ev435NM/+9vW1llp67LoCIZ6GPvPyLyWQ2963LU
-----BEGIN RSA PRIVATE KEY----
1frYns5AI Lbj2t8XnodtR3GWXbDEOMAH/ZLTb9hR9x1I F2gQK17gOOnFN9LuB830
AQABAOIBAGUYu466V441TOW1mec95XfVoLRO2FgWAzZ2bOrHWqOpLpcXFpw97
Wz6PuEvLyoPLpv2XXs Fab7eZ8mpL8ni+kI9RR8UZPpyMXRBXTg+6hxbYTR1mzM/p
UJenZulwUgkiD5 d5 f LXI+/W4zOTWAev4fKKJdgs1Xep3tebOZGdsqdutfLk+AD/hzH
Q04+XGCQNiRJ7vh5qlljpDXNNZFd/ddraM7YjQtpOBI5o/mRni8VE annrxdsmaP3RE
RtezHBIQE7RDkrEmCozhZ1TNdBm07+RtXOZUPAiWKiJXvk=pPjbAoGAP/4to1C5i/X2
50AJgoSf56xZUHe4A1ncfzH61bhpgpeUTIPGWnXEOsWrzRtjiptLk1AaUnTi99PU6u9hB
MI IE ogIBAAKCAQE Apd1]Zj7IR5COzo1UHiUvZmBmz7mxmLAdS+C3IGMIgN5Lhyci
735L9VJ9uIWraJmPkGzY as Mv7mZRR158T7z3fxB6bVVwIDE1qoFyAbMMjOz6NFh/X
0w6qB6iyd5PASt BgJ7w5J1u+5hifBUL9d2Nu7o/x5sMHNM3BMU2+PqTk89FFs AlLFm
6Dk5nYe95gNLOsWr1ZP+IDDUGN/MEYxa9fH+4P OT
----END RSA PRIVATE KEY-----
certificate-Notepad.txt - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE---
MIIGdzCCBF+gAwIBAgIQWvx1AEmEB4om30tTtQ3rEDANBgkqhkiG9yb1NTTDE qMCg
w@BAQWFADBLMQSICOYDVQQGEWJBVDEOMA4GA1UE ChMHWmVSktwHUUOUi
GALUE AxMhwmVyb1NTTCBSUOEgRG9tYWlul FNLY3VEVMBMGA1UE Ai24h2YhZf1R
yZSBTaXR1IENBMB4XDTIZMTIWNDAWMDAWMFoXDTI0MDMWMZIZNTk 1OVaFzUJ
Oz6NFh/Xd2Nu7o50AJg1AaUnTi99PU6u9hBew6qB6iyd5PAStBg37w5J1u+5hifBUL9
nRCKP9/cO12TyiYKWnb3+mLyFRlmMKOq0z8IgGP9/7s8PxHa3Au+g012D558rT40rG
enZuwUgkID5d5fLXI+/W4zOTwAev4fKKJdqs1Xep3tebozGdsqduqwfefTLVpSLM3Mj
XMMYXJtYXR1cmEub251MIIBIjANBgkqhkiG9wOBAQE FAAOCAQ8AMIIBCgKCA
QE Apd13Zj7IR5COzo1UHiUvZmBmz7mxmLAdS+C3IGMIgN5 LhyciE 1qoFyAbM
osfS6xZUHe4A1ncfzH61bhPgpeUTIPGWnXEOsWrzRtjiptLk
-END CERTIFICATE-----
private-Notepad.txt - Notepad
File Edit Format View Help