

A nighttime photograph of a city bridge and towers, likely in Prague, with a purple overlay. The bridge is illuminated with warm lights, and the towers have distinctive conical roofs. The background shows city buildings and a river with light trails from traffic.

Apache httpd and TLS/SSL certificates validation Jean-Frederic Clere

APACHECON Europe

Oct. 22-24, 2019

What I will cover

- TLS and certificates/keys (clients and servers)
 - Basics
- Client certificates OCSP responder or CRL.
- Servers certificates
 - Signed by CA, let's encrypt for example
 - mod_md to automate renewal
 - mod_md2 and OCSP stapling
- Demos
- Questions?

Who I am

Jean-Frederic Clere

Red Hat

Years writing JAVA code and server software

Tomcat committer since 2001

Doing OpenSource since 1999

Cyclist/Runner etc

Lived 15 years in Spain (Barcelona)

Now in Neuchâtel (CH)

APACHECON Europe

Key and Certificate

- A pair:
 - You keep the key secret
 - You “publish” the certificate
 - You identify your self in the certificate

Certificate authority

Let's encrypt

- How it works.

Client Hello (TLS 1.3 Firefox)

Capturing from Loopback: lo

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port ea 8443 Expression...

No.	Time	Source	Destination	Protocol	Length	Info
19	5.8198897...	:::1	:::1	TCP	94	33790 → 8443 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=642544819 TSecr=0 WS=128
20	5.8199414...	:::1	:::1	TCP	94	8443 → 33790 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=65476 SACK_PERM=1 TSval=642544819 TSecr=642544819 WS=128
21	5.8199675...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=642544819 TSecr=642544819
22	5.8230792...	:::1	:::1	TLSv1.3	699	Client Hello
23	5.8231215...	:::1	:::1	TCP	86	8443 → 33790 [ACK] Seq=1 Ack=614 Win=64896 Len=0 TSval=642544822 TSecr=642544822
24	5.8246183...	:::1	:::1	TLSv1.3	311	Server Hello, Change Cipher Spec, Application Data
25	5.8246540...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=614 Ack=226 Win=65408 Len=0 TSval=642544823 TSecr=642544823
26	5.8258582...	:::1	:::1	TLSv1.3	150	Change Cipher Spec, Application Data
27	5.8258887...	:::1	:::1	TCP	86	8443 → 33790 [ACK] Seq=226 Ack=678 Win=65536 Len=0 TSval=642544825 TSecr=642544825
28	5.8261749...	:::1	:::1	TLSv1.3	341	Application Data
29	5.8261971...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=678 Ack=481 Win=65408 Len=0 TSval=642544825 TSecr=642544825

Internet Protocol Version 6, Src: :::1, Dst: :::1

Transmission Control Protocol, Src Port: 33790, Dst Port: 8443, Seq: 1, Ack: 1, Len: 613

Transport Layer Security

- TLsv1.3 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 608
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 604
 - Version: TLS 1.2 (0x0303)
 - Random: 3d932c315865d56ff3d7f1cba47fc60347c250f7bda206f5...
 - Session ID Length: 32
 - Session ID: 972a5687df4419887b52430eb231f7fa4103534a07a9afa4...
 - Cipher Suites Length: 34
 - Cipher Suites (17 suites)
 - Compression Methods Length: 1

0000 00 00 00 00 00 00 00 00 00 00 00 86 dd 60 01

Loopback: lo: <live capture in progress>

Packets: 142 · Displayed: 142 (100.0%) Profile: Default

Server Hello (Tomcat)

Capturing from Loopback: lo

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port eq 8443

No.	Time	Source	Destination	Protocol	Length	Info
19	5.8198897...	:::1	:::1	TCP	94	33790 → 8443 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=642544819 TSecr=0 WS=128
20	5.8199414...	:::1	:::1	TCP	94	8443 → 33790 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=65476 SACK_PERM=1 TSval=642544819 TSecr=642544819 WS=128
21	5.8199675...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=642544819 TSecr=642544819
22	5.8230792...	:::1	:::1	TLSv1.3	699	Client Hello
23	5.8231215...	:::1	:::1	TCP	86	8443 → 33790 [ACK] Seq=1 Ack=614 Win=64896 Len=0 TSval=642544822 TSecr=642544822
24	5.8246183...	:::1	:::1	TLSv1.3	311	Server Hello, Change Cipher Spec, Application Data, Application Data
25	5.8246540...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=614 Ack=226 Win=65408 Len=0 TSval=642544823 TSecr=642544823
26	5.8258582...	:::1	:::1	TLSv1.3	150	Change Cipher Spec, Application Data
27	5.8258887...	:::1	:::1	TCP	86	8443 → 33790 [ACK] Seq=226 Ack=678 Win=65536 Len=0 TSval=642544825 TSecr=642544825
28	5.8261749...	:::1	:::1	TLSv1.3	341	Application Data
29	5.8261971...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=678 Ack=481 Win=65408 Len=0 TSval=642544825 TSecr=642544825

Session ID: 972a5687df4419887b52430eb231f7fa4103534a07a9afa4...

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 52

- Extension: supported_versions (len=2)
- Extension: key_share (len=36)
- Extension: pre_shared_key (len=2)

▼ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

- Content Type: Change Cipher Spec (20)
- Version: TLS 1.2 (0x0303)
- Length: 1
- Change Cipher Spec Message

▼ TLSv1.3 Record Layer: Application Data Protocol: Application Data

- Opaque Type: Application Data (23)
- Version: TLS 1.2 (0x0303)
- Length: 23
- Encrypted Application Data: 6c536e9074d4ee20025e04c9728715d30468f9a18416c1

0000 00 00 00 00 00 00 00 00 00 00 00 00 00 86 dd 60 07

Loopback: lo: <live capture in progress>

Packets: 142 · Displayed: 142 (100.0%) Profile: Default

TLS 1.3 versus 1.2

tcp.port eq 8443

No.	Time	Source	Destination	Protocol	Length	Info
19	5.8198897...	:::1	:::1	TCP	94	33790 → 8443 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=642544819 TSecr=0 WS=128
20	5.8199414...	:::1	:::1	TCP	94	8443 → 33790 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=65476 SACK_PERM=1 TSval=642544819 TSecr=642544819 WS=128
21	5.8199675...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=642544819 TSecr=642544819
22	5.8230792...	:::1	:::1	TLSv1.3	699	Client Hello
23	5.8231215...	:::1	:::1	TCP	86	8443 → 33790 [ACK] Seq=1 Ack=614 Win=64896 Len=0 TSval=642544822 TSecr=642544822
24	5.8246183...	:::1	:::1	TLSv1.3	311	Server Hello, Change Cipher Spec, Application Data, Application Data
25	5.8246540...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=614 Ack=226 Win=65408 Len=0 TSval=642544823 TSecr=642544823
26	5.8258582...	:::1	:::1	TLSv1.3	150	Change Cipher Spec, Application Data
27	5.8258887...	:::1	:::1	TCP	86	8443 → 33790 [ACK] Seq=226 Ack=678 Win=65536 Len=0 TSval=642544825 TSecr=642544825
28	5.8261749...	:::1	:::1	TLSv1.3	341	Application Data
29	5.8261971...	:::1	:::1	TCP	86	33790 → 8443 [ACK] Seq=678 Ack=481 Win=65408 Len=0 TSval=642544825 TSecr=642544825

tcp.port eq 8443

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000...	:::1	:::1	TCP	94	34224 → 8443 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=644712968 TSecr=0 WS=128
2	0.0000205...	:::1	:::1	TCP	94	8443 → 34224 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=65476 SACK_PERM=1 TSval=644712968 TSecr=644712968 WS=128
3	0.0000369...	:::1	:::1	TCP	86	34224 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=644712968 TSecr=644712968
4	0.0066240...	:::1	:::1	TLSv1.2	324	Client Hello
5	0.0066408...	:::1	:::1	TCP	86	8443 → 34224 [ACK] Seq=1 Ack=239 Win=65280 Len=0 TSval=644712974 TSecr=644712974
6	0.0077810...	:::1	:::1	TLSv1.2	2528	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7	0.0077927...	:::1	:::1	TCP	86	34224 → 8443 [ACK] Seq=239 Ack=2443 Win=63744 Len=0 TSval=644712975 TSecr=644712975
8	0.0083821...	:::1	:::1	TLSv1.2	179	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9	0.0083977...	:::1	:::1	TCP	86	8443 → 34224 [ACK] Seq=2443 Ack=332 Win=65536 Len=0 TSval=644712976 TSecr=644712976
10	0.0085280...	:::1	:::1	TLSv1.2	137	Change Cipher Spec, Encrypted Handshake Message
11	0.0085357...	:::1	:::1	TCP	86	34224 → 8443 [ACK] Seq=332 Ack=2494 Win=65536 Len=0 TSval=644712976 TSecr=644712976
12	0.0086760...	:::1	:::1	TLSv1.2	193	Application Data
13	0.0086847...	:::1	:::1	TCP	86	8443 → 34224 [ACK] Seq=2494 Ack=439 Win=65536 Len=0 TSval=644712976 TSecr=644712976
14	0.0111393...	:::1	:::1	TLSv1.2	8307	Application Data

TLS 1.3 versus 1.2 (look into 1.2!)

tcd.bort ed 8443

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000...	:::1	:::1	TCP	94	34224 → 8443 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=644712968 TSecr=0 WS=128
2	0.0000205...	:::1	:::1	TCP	94	8443 → 34224 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=65476 SACK_PERM=1 TSval=644712968 TSecr=644712968 WS=128
3	0.0000369...	:::1	:::1	TCP	86	34224 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=644712968 TSecr=644712968
4	0.0066240...	:::1	:::1	TLSv1.2	324	Client Hello
5	0.0066408...	:::1	:::1	TCP	86	8443 → 34224 [ACK] Seq=1 Ack=239 Win=65280 Len=0 TSval=644712974 TSecr=644712974
6	0.0077810...	:::1	:::1	TLSv1.2	2528	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7	0.0077927...	:::1	:::1	TCP	86	34224 → 8443 [ACK] Seq=239 Ack=2443 Win=63744 Len=0 TSval=644712975 TSecr=644712975
8	0.0083821...	:::1	:::1	TLSv1.2	179	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9	0.0083977...	:::1	:::1	TCP	86	8443 → 34224 [ACK] Seq=2443 Ack=332 Win=65536 Len=0 TSval=644712976 TSecr=644712976
10	0.0085280...	:::1	:::1	TLSv1.2	137	Change Cipher Spec, Encrypted Handshake Message
11	0.0085357...	:::1	:::1	TCP	86	34224 → 8443 [ACK] Seq=332 Ack=2494 Win=65536 Len=0 TSval=644712976 TSecr=644712976
12	0.0086760...	:::1	:::1	TLSv1.2	193	Application Data
13	0.0086847...	:::1	:::1	TCP	86	8443 → 34224 [ACK] Seq=2494 Ack=439 Win=65536 Len=0 TSval=644712976 TSecr=644712976
14	0.0111393...	:::1	:::1	TLSv1.2	8307	Application Data

▼ Handshake Protocol: Certificate

- Handshake Type: Certificate (11)
- Length: 2049
- Certificates Length: 2046
- ▼ Certificates (2046 bytes)

 - Certificate Length: 1058
 - ▶Certificate: 3082041e30820306a003020102020900b94877ebce531bc6... (pkcs-9-at-emailAddress=jfclere@gmail.com,id-at-commonName=localhost,id-at-organizationalUnitName=ldap server,id-at-...
 - Certificate Length: 982
 - ▶Certificate: 308203d2308202baa003020102020900b94877ebce531bb1... (pkcs-9-at-emailAddress=jfclere@gmail.com,id-at-commonName=jfcpcc,id-at-organizationalUnitName=Test Neuchatel,id-at-o...

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 300
- ▼ Handshake Protocol: Server Key Exchange

HTTPd / Configuration / Basic

- httpd.conf:

Listen 8888

<VirtualHost _default_:8888>

SSLEngine on

SSLCertificateFile

"/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newcert.pem"

SSLCertificateKeyFile

"/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newkey.pem"

SSLCACertificateFile "/etc/pki/CA/cacert.pem"

SSLOptions +StdEnvVars -ExportCertData

ScriptAlias /cgi-bin/ "/home/jfclere/APACHE/cgi-bin/"

</VirtualHost>

Client Certificate required

- httpd.conf:

```
Listen 8889
```

```
<VirtualHost _default_:8889>
```

```
SSLEngine on
```

```
SSLCertificateFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newcert.pem"
```

```
SSLCertificateKeyFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newkey.pem"
```

```
SSLCACertificateFile "/etc/pki/CA/cacert.pem"
```

```
SSLOptions +StdEnvVars -ExportCertData
```

```
ScriptAlias /cgi-bin/ "/home/jfclere/APACHE/cgi-bin/"
```

```
SSLVerifyClient require
```

```
SSLVerifyDepth 1
```

```
</VirtualHost>
```

With revocation in a file.

- httpd.conf:

```
Listen 8890
```

```
<VirtualHost _default_:8890>
```

```
SSLEngine on
```

```
SSLCertificateFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newcert.pem"
```

```
SSLCertificateKeyFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newkey.pem"
```

```
SSLCACertificateFile "/etc/pki/CA/cacert.pem"
```

```
SSLOptions +StdEnvVars -ExportCertData
```

```
ScriptAlias /cgi-bin/ "/home/jfclere/APACHE/cgi-bin/"
```

```
SSLVerifyClient require
```

```
SSLVerifyDepth 1
```

```
SSLCARevocationCheck leaf
```

```
SSLCARevocationFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/crl_01.pem"
```

```
</VirtualHost>
```

With OCSP responder for revocation.

- httpd.conf:

```
Listen 8891
```

```
<VirtualHost _default_:8891>
```

```
SSLEngine on
```

```
SSLCertificateFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newcert.pem"
```

```
SSLCertificateKeyFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newkey.pem"
```

```
SSLCACertificateFile "/etc/pki/CA/cacert.pem"
```

```
SSLOptions +StdEnvVars -ExportCertData
```

```
ScriptAlias /cgi-bin/ "/home/jfclere/APACHE/cgi-bin/"
```

```
SSLVerifyClient require
```

```
SSLVerifyDepth 1
```

```
SSLOCSPEnable on
```

```
SSLOCSPEndpoint http://jfcpc:2560/
```

```
SSLOCSPOverrideResponder on
```

```
</VirtualHost>
```

Using “OCSP responder” in certificate

- httpd.conf:

```
Listen 8892
```

```
<VirtualHost _default_:8892>
```

```
SSLEngine on
```

```
SSLCertificateFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newcert.pem"
```

```
SSLCertificateKeyFile "/home/jfclere/NOTES/APACHECONNA2019/httpdssl/jfcpc_newkey.pem"
```

```
SSLCACertificateFile "/etc/pki/CA/cacert.pem"
```

```
SSLOptions +StdEnvVars -ExportCertData
```

```
ScriptAlias /cgi-bin/ "/home/jfclere/APACHE/cgi-bin/"
```

```
SSLVerifyClient require
```

```
SSLVerifyDepth 1
```

```
SSLOCSPEnable on
```

```
</VirtualHost>
```

Servers!!!

- Let's look to the server certificates:
 - **Validation like for the client certificates**
 - **Signed by CA**
 - **OCSP**
 - **stapling**

Let's Encrypt!

- See [Let's encrypt](#):
 - Signed certificates valid for 90 days.
 - Challenge to prove you own the host/domain.
 - ~~HTTP/DNS/TLS-SNI/TLS-ALPN~~
 - Renewal: certbot renew
 - Renewal: mod_md
 - OCSP stapling

Certbot config

```
<VirtualHost _default_:443>
```

```
ServerName jfclere.noip.me:443
```

```
SSLEngine on
```

```
SSLCertificateFile /etc/letsencrypt/live/jfclere.noip.me/fullchain.pem
```

```
SSLCertificateKeyFile /etc/letsencrypt/live/jfclere.noip.me/privkey.pem
```

```
Include /etc/letsencrypt/options-ssl-apache.conf
```

```
</VirtualHost>
```


mod_md

```
<VirtualHost _default_:443>
```

```
ServerName jfclere.noip.me:443
```

```
SSLEngine on
```

```
</VirtualHost>
```

```
ServerAdmin jfclere@gmail.com
```

```
MDCertificateAgreement https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf
```

```
MDomain jfclere.noip.me
```

- **Note you have to restart the server the first time:**

 - The Managed Domain jfclere.noip.me has been setup and changes will be activated on next (graceful) server restart.

- **SELinux:** `setsebool -P httpd_can_network_connect 1`

stapling

```
MDMUSTStaple (mod_md)
```

```
MDMUSTStaple On
```

```
SSLUSEStapling (mod_ssl in ssl.conf)
```

```
SSLStaplingCache shmcb:/run/httpd/sslstaplingcache(512000)
```

```
<VirtualHost _default_:443>
```

```
SSLUSEStapling On
```

```
...
```

```
openssl s_client -connect jfclere.noip.me:443 -status
```

```
OCSP response:
```

```
=====
```

```
OCSP Response Data:
```

```
OCSP Response Status: successful (0x0)
```

```
Response Type: Basic OCSP Response
```

```
Version: 1 (0x0)
```

```
Responder Id: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
```

```
Produced At: Sep 3 14:28:00 2019 GMT
```

ACME V2

Not backward compatible with V1

Requires `mod_md 2.x` `mod_md v2.1.5 (beta)`

let's encrypt V2 services [[Test for V2 clients.](#)]

Soon in httpd

V1 will be sunset “ at some point in the future”.

Questions?

Thank you!

- jfclere@gmail.com
- users@httpd.apache.org
- dev@httpd.apache.org
- <https://github.com/apache/httpd>
- <https://github.com/jfclere/AC2014scripts/blob/master/httpdssl.txt>
: commands for demos.

THANK YOU

Jean-Frederic Clere

@jfclere

jfclere@gmail.com