```
1 /Library/Java/JavaVirtualMachines/jdk-17.jdk/
  Contents/Home/bin/java -Djavax.net.debug=all -
  javaagent:/Applications/IntelliJ IDEA CE.app/
  Contents/lib/idea_rt.jar=55376:/Applications/
  IntelliJ IDEA CE.app/Contents/bin -Dfile.encoding=
  UTF-8 -classpath /Users/madhu/work/Java Projects/
  redis-projects/redis-guard/target/classes:/Users/
  madhu/.m2/repository/org/springframework/boot/
  spring-boot-starter-data-redis/3.3.5/spring-boot-
  starter-data-redis-3.3.5.jar:/Users/madhu/.m2/
  repository/org/springframework/boot/spring-boot-
  starter/3.3.5/spring-boot-starter-3.3.5.jar:/Users/
  madhu/.m2/repository/org/springframework/boot/
  spring-boot/3.3.5/spring-boot-3.3.5.jar:/Users/
  madhu/.m2/repository/org/springframework/boot/
  spring-boot-autoconfigure/3.3.5/spring-boot-
  autoconfigure-3.3.5.jar:/Users/madhu/.m2/repository
  /org/springframework/boot/spring-boot-starter-
  logging/3.3.5/spring-boot-starter-logging-3.3.5.jar
  :/Users/madhu/.m2/repository/ch/qos/logback/logback
  -classic/1.5.11/logback-classic-1.5.11.jar:/Users/
  madhu/.m2/repository/ch/qos/logback/logback-core/1.
  5.11/logback-core-1.5.11.jar:/Users/madhu/.m2/
  repository/org/apache/logging/log4j/log4j-to-slf4j/
  2.23.1/log4j-to-slf4j-2.23.1.jar:/Users/madhu/.m2/
  repository/org/apache/logging/log4j/log4j-api/2.23.
  1/log4j-api-2.23.1.jar:/Users/madhu/.m2/repository/
  org/slf4j/jul-to-slf4j/2.0.16/jul-to-slf4j-2.0.16.
  jar:/Users/madhu/.m2/repository/jakarta/annotation/
  jakarta.annotation-api/2.1.1/jakarta.annotation-api
  -2.1.1.jar:/Users/madhu/.m2/repository/org/yaml/
  snakeyaml/2.2/snakeyaml-2.2.jar:/Users/madhu/.m2/
  repository/io/lettuce/lettuce-core/6.3.2.RELEASE/
  lettuce-core-6.3.2.RELEASE.jar:/Users/madhu/.m2/
  repository/io/netty/netty-common/4.1.114.Final/
  netty-common-4.1.114.Final.jar:/Users/madhu/.m2/
  repository/io/netty/netty-handler/4.1.114.Final/
  netty-handler-4.1.114.Final.jar:/Users/madhu/.m2/
  repository/io/netty/netty-resolver/4.1.114.Final/
  netty-resolver-4.1.114.Final.jar:/Users/madhu/.m2/
  repository/io/netty/netty-buffer/4.1.114.Final/
```

```
1 netty-buffer-4.1.114.Final.jar:/Users/madhu/.m2/
  repository/io/netty/netty-transport-native-unix-
  common/4.1.114.Final/netty-transport-native-unix-
  common-4.1.114.Final.jar:/Users/madhu/.m2/
  repository/io/netty/netty-codec/4.1.114.Final/netty
  -codec-4.1.114.Final.jar:/Users/madhu/.m2/
  repository/io/netty/netty-transport/4.1.114.Final/
  netty-transport-4.1.114.Final.jar:/Users/madhu/.m2/
  repository/io/projectreactor/reactor-core/3.6.11/
  reactor-core-3.6.11.jar:/Users/madhu/.m2/repository
  /org/reactivestreams/reactive-streams/1.0.4/
  reactive-streams-1.0.4.jar:/Users/madhu/.m2/
  repository/org/springframework/data/spring-data-
  redis/3.3.5/spring-data-redis-3.3.5.jar:/Users/
  madhu/.m2/repository/org/springframework/data/
  spring-data-keyvalue/3.3.5/spring-data-keyvalue-3.3
  .5.jar:/Users/madhu/.m2/repository/org/
  springframework/data/spring-data-commons/3.3.5/
  spring-data-commons-3.3.5.jar:/Users/madhu/.m2/
  repository/org/springframework/spring-tx/6.1.14/
  spring-tx-6.1.14.jar:/Users/madhu/.m2/repository/
  org/springframework/spring-oxm/6.1.14/spring-oxm-6.
  1.14.jar:/Users/madhu/.m2/repository/org/
  springframework/spring-aop/6.1.14/spring-aop-6.1.14
  .jar:/Users/madhu/.m2/repository/org/
  springframework/spring-context-support/6.1.14/
  spring-context-support-6.1.14.jar:/Users/madhu/.m2/
  repository/org/slf4j/slf4j-api/2.0.16/slf4j-api-2.0
  .16.jar:/Users/madhu/.m2/repository/org/
  springframework/boot/spring-boot-starter-web/3.3.5/
  spring-boot-starter-web-3.3.5.jar:/Users/madhu/.m2/
  repository/org/springframework/boot/spring-boot-
  starter-json/3.3.5/spring-boot-starter-json-3.3.5.
  jar:/Users/madhu/.m2/repository/com/fasterxml/
  jackson/core/jackson-databind/2.17.2/jackson-
  databind-2.17.2.jar:/Users/madhu/.m2/repository/com
  /fasterxml/jackson/core/jackson-annotations/2.17.2/
  jackson-annotations-2.17.2.jar:/Users/madhu/.m2/
  repository/com/fasterxml/jackson/core/jackson-core/
  2.17.2/jackson-core-2.17.2.jar:/Users/madhu/.m2/
  repository/com/fasterxml/jackson/datatype/jackson-
```

```
1 datatype-jdk8/2.17.2/jackson-datatype-jdk8-2.17.2.
  jar:/Users/madhu/.m2/repository/com/fasterxml/
  jackson/datatype/jackson-datatype-jsr310/2.17.2/
  jackson-datatype-jsr310-2.17.2.jar:/Users/madhu/.m2
  /repository/com/fasterxml/jackson/module/jackson-
  module-parameter-names/2.17.2/jackson-module-
  parameter-names-2.17.2.jar:/Users/madhu/.m2/
  repository/org/springframework/boot/spring-boot-
  starter-tomcat/3.3.5/spring-boot-starter-tomcat-3.3
  .5.jar:/Users/madhu/.m2/repository/org/apache/
  tomcat/embed/tomcat-embed-core/10.1.31/tomcat-embed
  -core-10.1.31.jar:/Users/madhu/.m2/repository/org/
  apache/tomcat/embed/tomcat-embed-el/10.1.31/tomcat-
  embed-el-10.1.31.jar:/Users/madhu/.m2/repository/
  org/apache/tomcat/embed/tomcat-embed-websocket/10.1
  .31/tomcat-embed-websocket-10.1.31.jar:/Users/madhu
  /.m2/repository/org/springframework/spring-web/6.1.
  14/spring-web-6.1.14.jar:/Users/madhu/.m2/
  repository/org/springframework/spring-beans/6.1.14/
  spring-beans-6.1.14.jar:/Users/madhu/.m2/repository
  /io/micrometer/micrometer-observation/1.13.6/
  micrometer-observation-1.13.6.jar:/Users/madhu/.m2/
  repository/io/micrometer/micrometer-commons/1.13.6/
  micrometer-commons-1.13.6.jar:/Users/madhu/.m2/
  repository/org/springframework/spring-webmvc/6.1.14
  /spring-webmvc-6.1.14.jar:/Users/madhu/.m2/
  repository/org/springframework/spring-context/6.1.
  14/spring-context-6.1.14.jar:/Users/madhu/.m2/
  repository/org/springframework/spring-expression/6.
  1.14/spring-expression-6.1.14.jar:/Users/madhu/.m2/
  repository/org/projectlombok/lombok/1.18.34/lombok-
  1.18.34.jar:/Users/madhu/.m2/repository/jakarta/xml
  /bind/jakarta.xml.bind-api/4.0.2/jakarta.xml.bind-
  api-4.0.2.jar:/Users/madhu/.m2/repository/jakarta/
  activation/jakarta.activation-api/2.1.3/jakarta.
  activation-api-2.1.3.jar:/Users/madhu/.m2/
  repository/org/springframework/spring-core/6.1.14/
  spring-core-6.1.14.jar:/Users/madhu/.m2/repository/
  org/springframework/spring-jcl/6.1.14/spring-jcl-6.
  1.14.jar io.madhu.redisGuard.RedisGuardApplication
2
```

```
 3   .   ____          _            __ _ _
 4  /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
 5 ( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 6  \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
 7   '  |____| .__|_| |_|_| |_\__, | / / / /
 8  =========|_|==============|___/=/_/_/_/
 9
10  :: Spring Boot ::                (v3.3.5)
11
12 2024-11-01T15:06:02.318+08:00  INFO 29986 --- [
   redis-guard] [           main] i.m.redisGuard.
   RedisGuardApplication     : Starting
   RedisGuardApplication using Java 17.0.10 with PID
   29986 (/Users/madhu/work/Java Projects/redis-
   projects/redis-guard/target/classes started by
   madhu in /Users/madhu/work/Java Projects/redis-
   projects/redis-guard)
13 2024-11-01T15:06:02.320+08:00  INFO 29986 --- [
   redis-guard] [           main] i.m.redisGuard.
   RedisGuardApplication     : No active profile set,
   falling back to 1 default profile: "default"
14 2024-11-01T15:06:02.547+08:00  INFO 29986 --- [
   redis-guard] [           main] .s.d.r.c.
   RepositoryConfigurationDelegate : Multiple Spring
   Data modules found, entering strict repository
   configuration mode
15 2024-11-01T15:06:02.549+08:00  INFO 29986 --- [
   redis-guard] [           main] .s.d.r.c.
   RepositoryConfigurationDelegate : Bootstrapping
   Spring Data Redis repositories in DEFAULT mode.
16 2024-11-01T15:06:02.563+08:00  INFO 29986 --- [
   redis-guard] [           main] .s.d.r.c.
   RepositoryConfigurationDelegate : Finished Spring
   Data repository scanning in 7 ms. Found 0 Redis
   repository interfaces.
17 2024-11-01T15:06:02.730+08:00  INFO 29986 --- [
   redis-guard] [           main] o.s.b.w.embedded.
   tomcat.TomcatWebServer  : Tomcat initialized with
   port 8080 (http)
18 2024-11-01T15:06:02.736+08:00  INFO 29986 --- [
   redis-guard] [           main] o.apache.catalina.
```

```
core.StandardService   : Starting service [Tomcat]
2024-11-01T15:06:02.736+08:00  INFO 29986 --- [
   redis-guard] [           main] o.apache.catalina.
   core.StandardEngine    : Starting Servlet engine: [
   Apache Tomcat/10.1.31]
2024-11-01T15:06:02.761+08:00  INFO 29986 --- [
   redis-guard] [           main] o.a.c.c.C.[Tomcat].[
   localhost].[/]       : Initializing Spring embedded
    WebApplicationContext
2024-11-01T15:06:02.762+08:00  INFO 29986 --- [
   redis-guard] [           main] w.s.c.
   ServletWebServerApplicationContext : Root
   WebApplicationContext: initialization completed in
   421 ms
2024-11-01T15:06:03.050+08:00  INFO 29986 --- [
   redis-guard] [           main] o.s.b.w.embedded.
   tomcat.TomcatWebServer  : Tomcat started on port
   8080 (http) with context path '/'
2024-11-01T15:06:03.055+08:00  INFO 29986 --- [
   redis-guard] [           main] i.m.redisGuard.
   RedisGuardApplication     : Started
   RedisGuardApplication in 0.901 seconds (process
   running for 1.045)
javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.198 SGT|SSLContextImpl.java:423
   |System property jdk.tls.client.cipherSuites is set
    to 'null'
javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.199 SGT|SSLContextImpl.java:423
   |System property jdk.tls.server.cipherSuites is set
    to 'null'
javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.215 SGT|SSLCipher.java:466|jdk.
   tls.keyLimits:  entry = AES/GCM/NoPadding KeyUpdate
    2^37. AES/GCM/NOPADDING:KEYUPDATE = 137438953472
javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.216 SGT|SSLCipher.java:466|jdk.
   tls.keyLimits:  entry =  ChaCha20-Poly1305
   KeyUpdate 2^37. CHACHA20-POLY1305:KEYUPDATE =
   137438953472
javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
```

```
28 2024-11-01 15:06:03.220 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
29 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.220 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
30 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.220 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
31 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.220 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
32 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.220 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
33 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.220 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
34 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.220 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
35 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.220 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
36 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.220 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
37 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.220 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
38 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.221 SGT|SSLContextImpl.java:397
```

```
38 |Ignore disabled cipher suite:
   TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
39 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.221 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
40 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.221 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   SSL_RSA_WITH_3DES_EDE_CBC_SHA
41 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.221 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_RSA_WITH_3DES_EDE_CBC_SHA
42 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.221 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_DH_anon_WITH_AES_256_GCM_SHA384
43 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.221 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_DH_anon_WITH_AES_256_GCM_SHA384
44 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.221 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_DH_anon_WITH_AES_128_GCM_SHA256
45 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.221 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_DH_anon_WITH_AES_128_GCM_SHA256
46 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.221 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_DH_anon_WITH_AES_256_CBC_SHA256
47 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.221 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_DH_anon_WITH_AES_256_CBC_SHA256
48 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.221 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
```

```
48 TLS_ECDH_anon_WITH_AES_256_CBC_SHA
49 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.221 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_anon_WITH_AES_256_CBC_SHA
50 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.221 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_DH_anon_WITH_AES_256_CBC_SHA
51 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_DH_anon_WITH_AES_256_CBC_SHA
52 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.222 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_DH_anon_WITH_AES_128_CBC_SHA256
53 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_DH_anon_WITH_AES_128_CBC_SHA256
54 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.222 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDH_anon_WITH_AES_128_CBC_SHA
55 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_anon_WITH_AES_128_CBC_SHA
56 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.222 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_DH_anon_WITH_AES_128_CBC_SHA
57 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_DH_anon_WITH_AES_128_CBC_SHA
58 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.222 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
```

```
59 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
60 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.222 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
61 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
62 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.222 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
63 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
64 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.222 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDHE_RSA_WITH_RC4_128_SHA
65 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.222 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDHE_RSA_WITH_RC4_128_SHA
66 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   SSL_RSA_WITH_RC4_128_SHA
67 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
   11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_RSA_WITH_RC4_128_SHA
68 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:397
   |Ignore disabled cipher suite:
   TLS_ECDH_ECDSA_WITH_RC4_128_SHA
69 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024-
```

```
69 11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_ECDSA_WITH_RC4_128_SHA
70 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   TLS_ECDH_RSA_WITH_RC4_128_SHA
71 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_RSA_WITH_RC4_128_SHA
72 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_RSA_WITH_RC4_128_MD5
73 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_RSA_WITH_RC4_128_MD5
74 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   TLS_ECDH_anon_WITH_RC4_128_SHA
75 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   TLS_ECDH_anon_WITH_RC4_128_SHA
76 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_DH_anon_WITH_RC4_128_MD5
77 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_DH_anon_WITH_RC4_128_MD5
78 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_RSA_WITH_DES_CBC_SHA
79 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
```

```
79 Ignore unsupported cipher suite:
   SSL_RSA_WITH_DES_CBC_SHA
80 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_DHE_RSA_WITH_DES_CBC_SHA
81 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.223 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_DHE_RSA_WITH_DES_CBC_SHA
82 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.223 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_DHE_DSS_WITH_DES_CBC_SHA
83 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_DHE_DSS_WITH_DES_CBC_SHA
84 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_DH_anon_WITH_DES_CBC_SHA
85 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_DH_anon_WITH_DES_CBC_SHA
86 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
87 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
   SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
88 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
   2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
   397|Ignore disabled cipher suite:
   SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
89 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
   -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
   Ignore unsupported cipher suite:
```

```
 89 SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
 90 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
 91 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
 92 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
 93 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
 94 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_RSA_EXPORT_WITH_RC4_40_MD5
 95 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_RSA_EXPORT_WITH_RC4_40_MD5
 96 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
 97 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
 98 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_RSA_WITH_NULL_SHA256
 99 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.224 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_RSA_WITH_NULL_SHA256
```

```
100 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.224 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDHE_ECDSA_WITH_NULL_SHA
101 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_ECDSA_WITH_NULL_SHA
102 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDHE_RSA_WITH_NULL_SHA
103 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_RSA_WITH_NULL_SHA
104 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_RSA_WITH_NULL_SHA
105 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_RSA_WITH_NULL_SHA
106 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_ECDSA_WITH_NULL_SHA
107 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_ECDSA_WITH_NULL_SHA
108 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_RSA_WITH_NULL_SHA
109 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_RSA_WITH_NULL_SHA
110 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
```

```
110 2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_anon_WITH_NULL_SHA
111 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_anon_WITH_NULL_SHA
112 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_RSA_WITH_NULL_MD5
113 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_RSA_WITH_NULL_MD5
114 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
115 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
116 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
117 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
118 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
119 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.225 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
120 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.225 SGT|SSLContextImpl.java:
```

```
120 397|Ignore disabled cipher suite:
    SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
121 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
122 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
123 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
124 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
125 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
126 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
127 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
128 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
129 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
130 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
```

```
130 TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
131 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
132 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
133 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
134 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
135 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
136 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
137 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
138 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
139 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
140 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.226 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
```

```
141 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.226 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
142 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.227 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
143 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.227 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
144 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.227 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
145 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.227 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
146 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.227 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
147 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.227 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
148 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.227 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
149 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.227 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
150 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.227 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
151 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
```

```
151 -11-01 15:06:03.227 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
152 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.227 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
153 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.227 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
154 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.227 SGT|SSLContextImpl.java:
    397|Ignore disabled cipher suite:
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
155 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|2024
    -11-01 15:06:03.227 SGT|SSLContextImpl.java:406|
    Ignore unsupported cipher suite:
    SSL_RSA_WITH_3DES_EDE_CBC_SHA
156 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.228 SGT|TrustStoreManager.java
    :162|Inaccessible trust store: /Library/Java/
    JavaVirtualMachines/jdk-17.jdk/Contents/Home/lib/
    security/jssecacerts
157 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.228 SGT|TrustStoreManager.java
    :113|trustStore is: /Library/Java/
    JavaVirtualMachines/jdk-17.jdk/Contents/Home/lib/
    security/cacerts
158 trustStore type is: pkcs12
159 trustStore provider is:
160 the last modified time is: Fri Nov 01 15:05:44 SGT
     2024
161 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.228 SGT|TrustStoreManager.java
    :334|Reload the trust store
162 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.240 SGT|TrustStoreManager.java
    :342|Reload trust certs
163 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
    2024-11-01 15:06:03.241 SGT|TrustStoreManager.java
```

```
:347|Reloaded 107 trust certs
javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|2024-11-01 15:06:03.273 SGT|X509TrustManagerImpl.java:82|adding as trusted certificates (
  "certificate" : {
    "version"            : "v3",
    "serial number"      : "00A68B79290000000050D091F9",
    "signature algorithm": "SHA384withECDSA",
    "issuer"             : "CN=Entrust Root Certification Authority - EC1, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US",
    "not before"         : "2012-12-18 23:25:36.000 SGT",
    "not  after"         : "2037-12-18 23:55:36.000 SGT",
    "subject"            : "CN=Entrust Root Certification Authority - EC1, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US",
    "subject public key" : "EC",
    "extensions"         : [
      {
        ObjectId: 2.5.29.19 Criticality=true
        BasicConstraints:[
          CA:true
          PathLen: no limit
        ]
      },
      {
        ObjectId: 2.5.29.15 Criticality=true
        KeyUsage [
          Key_CertSign
          Crl_Sign
        ]
      },
      {
        ObjectId: 2.5.29.14 Criticality=false
```

```
191         SubjectKeyIdentifier [
192         KeyIdentifier [
193         0000: B7 63 E7 1A DD 8D E9 08   A6 55 83
    A4 E0 6A 50 41  .c.......U...jPA
194         0010: 65 11 42 49
                                            e.BI
195         ]
196         ]
197       }
198     ]},
199   "certificate" : {
200     "version"            : "v3",
201     "serial number"      : "
    0CF08E5C0816A5AD427FF0EB271859D0",
202     "signature algorithm": "SHA1withRSA",
203     "issuer"             : "CN=SecureTrust CA, O=
    SecureTrust Corporation, C=US",
204     "not before"         : "2006-11-08 03:31:18.
    000 SGT",
205     "not  after"         : "2030-01-01 03:40:55.
    000 SGT",
206     "subject"            : "CN=SecureTrust CA, O=
    SecureTrust Corporation, C=US",
207     "subject public key" : "RSA",
208     "extensions"         : [
209       {
210         ObjectId: 1.3.6.1.4.1.311.20.2 Criticality
    =false
211       },
212       {
213         ObjectId: 1.3.6.1.4.1.311.21.1 Criticality
    =false
214       },
215       {
216         ObjectId: 2.5.29.19 Criticality=true
217         BasicConstraints:[
218           CA:true
219           PathLen: no limit
220         ]
221       },
222       {
```

```
223         ObjectId: 2.5.29.31 Criticality=false
224         CRLDistributionPoints [
225           [DistributionPoint:
226              [URIName: http://crl.securetrust.com/
    STCA.crl]
227         ]]
228       },
229       {
230         ObjectId: 2.5.29.15 Criticality=false
231         KeyUsage [
232           DigitalSignature
233           Key_CertSign
234           Crl_Sign
235         ]
236       },
237       {
238         ObjectId: 2.5.29.14 Criticality=false
239         SubjectKeyIdentifier [
240         KeyIdentifier [
241         0000: 42 32 B6 16 FA 04 FD FE   5D 4B 7A
    C3 FD F7 4C 40  B2......]Kz...L@
242         0010: 1D 5A 43 AF
                                                .ZC.
243         ]
244         ]
245       }
246     ]},
247   "certificate" : {
248     "version"            : "v3",
249     "serial number"      : "
    083BE056904246B1A1756AC95991C74A",
250     "signature algorithm": "SHA1withRSA",
251     "issuer"             : "CN=DigiCert Global
    Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
    ",
252     "not before"         : "2006-11-10 08:00:00.
    000 SGT",
253     "not  after"         : "2031-11-10 08:00:00.
    000 SGT",
254     "subject"            : "CN=DigiCert Global
    Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
```

```
",
    "subject public key" : "RSA",
    "extensions"         : [
      {
        ObjectId: 2.5.29.35 Criticality=false
        AuthorityKeyIdentifier [
        KeyIdentifier [
        0000: 03 DE 50 35 56 D1 4C BB   66 F0 A3
    E2 1B 1B C3 97  ..P5V.L.f.......
        0010: B2 3D D1 55
                                              .=.U
        ]
        ]
      },
      {
        ObjectId: 2.5.29.19 Criticality=true
        BasicConstraints:[
          CA:true
          PathLen: no limit
        ]
      },
      {
        ObjectId: 2.5.29.15 Criticality=true
        KeyUsage [
          DigitalSignature
          Key_CertSign
          Crl_Sign
        ]
      },
      {
        ObjectId: 2.5.29.14 Criticality=false
        SubjectKeyIdentifier [
        KeyIdentifier [
        0000: 03 DE 50 35 56 D1 4C BB   66 F0 A3
    E2 1B 1B C3 97  ..P5V.L.f.......
        0010: B2 3D D1 55
                                              .=.U
        ]
        ]
      }
    ]},
```

```
291   "certificate" : {
292     "version"            : "v3",
293     "serial number"      : "00",
294     "signature algorithm": "SHA256withRSA",
295     "issuer"             : "CN=Hellenic Academic
    and Research Institutions RootCA 2015, O=Hellenic
    Academic and Research Institutions Cert. Authority
    , L=Athens, C=GR",
296     "not before"         : "2015-07-07 18:11:21.
    000 SGT",
297     "not  after"         : "2040-06-30 18:11:21.
    000 SGT",
298     "subject"            : "CN=Hellenic Academic
    and Research Institutions RootCA 2015, O=Hellenic
    Academic and Research Institutions Cert. Authority
    , L=Athens, C=GR",
299     "subject public key" : "RSA",
300     "extensions"         : [
301       {
302         ObjectId: 2.5.29.19 Criticality=true
303         BasicConstraints:[
304           CA:true
305           PathLen: no limit
306         ]
307       },
308       {
309         ObjectId: 2.5.29.15 Criticality=true
310         KeyUsage [
311           Key_CertSign
312           Crl_Sign
313         ]
314       },
315       {
316         ObjectId: 2.5.29.14 Criticality=false
317         SubjectKeyIdentifier [
318         KeyIdentifier [
319         0000: 71 15 67 C8 C8 C9 BD 75   5D 72 D0
    38 18 6A 9D F3  q.g....u]r.8.j..
320         0010: 71 24 54 0B
                                            q$T.
321         ]
```

```
322         ]
323       }
324     ]},
325   "certificate" : {
326     "version"            : "v3",
327     "serial number"      : "
    445734245B81899B35F2CEB82B3B5BA726F07528",
328     "signature algorithm": "SHA256withRSA",
329     "issuer"             : "CN=QuoVadis Root CA 2
    G3, O=QuoVadis Limited, C=BM",
330     "not before"         : "2012-01-13 02:59:32.
    000 SGT",
331     "not  after"         : "2042-01-13 02:59:32.
    000 SGT",
332     "subject"            : "CN=QuoVadis Root CA 2
    G3, O=QuoVadis Limited, C=BM",
333     "subject public key" : "RSA",
334     "extensions"         : [
335       {
336         ObjectId: 2.5.29.19 Criticality=true
337         BasicConstraints:[
338           CA:true
339           PathLen: no limit
340         ]
341       },
342       {
343         ObjectId: 2.5.29.15 Criticality=true
344         KeyUsage [
345           Key_CertSign
346           Crl_Sign
347         ]
348       },
349       {
350         ObjectId: 2.5.29.14 Criticality=false
351         SubjectKeyIdentifier [
352         KeyIdentifier [
353         0000: ED E7 6F 76 5A BF 60 EC   49 5B C6
    A5 77 BB 72 16  ..ovZ.`.I[..w.r.
354         0010: 71 9B C4 3D
                                            q..=
355         ]
```

```
356         ]
357       }
358     ]},
359   "certificate" : {
360     "version"            : "v3",
361     "serial number"      : "
    059B1B579E8E2132E23907BDA777755C",
362     "signature algorithm": "SHA384withRSA",
363     "issuer"             : "CN=DigiCert Trusted
    Root G4, OU=www.digicert.com, O=DigiCert Inc, C=US
    ",
364     "not before"         : "2013-08-01 20:00:00.
    000 SGT",
365     "not  after"         : "2038-01-15 20:00:00.
    000 SGT",
366     "subject"            : "CN=DigiCert Trusted
    Root G4, OU=www.digicert.com, O=DigiCert Inc, C=US
    ",
367     "subject public key" : "RSA",
368     "extensions"         : [
369       {
370         ObjectId: 2.5.29.19 Criticality=true
371         BasicConstraints:[
372           CA:true
373           PathLen: no limit
374         ]
375       },
376       {
377         ObjectId: 2.5.29.15 Criticality=true
378         KeyUsage [
379           DigitalSignature
380           Key_CertSign
381           Crl_Sign
382         ]
383       },
384       {
385         ObjectId: 2.5.29.14 Criticality=false
386         SubjectKeyIdentifier [
387         KeyIdentifier [
388         0000: EC D7 E3 82 D2 71 5D 64   4C DF 2E
    67 3F E7 BA 98  .....q]dL..g?...
```

```
389         0010: AE 1C 0F 4F                                        ...O
390         ]
391         ]
392       }
393     ]},
394   "certificate" : {
395     "version"            : "v3",
396     "serial number"      : "
    18ACB56AFD69B6153A636CAFDAFAC4A1",
397     "signature algorithm": "SHA1withRSA",
398     "issuer"             : "CN=GeoTrust Primary
    Certification Authority, O=GeoTrust Inc., C=US",
399     "not before"         : "2006-11-27 08:00:00.
    000 SGT",
400     "not  after"         : "2036-07-17 07:59:59.
    000 SGT",
401     "subject"            : "CN=GeoTrust Primary
    Certification Authority, O=GeoTrust Inc., C=US",
402     "subject public key" : "RSA",
403     "extensions"         : [
404       {
405         ObjectId: 2.5.29.19 Criticality=true
406         BasicConstraints:[
407           CA:true
408           PathLen: no limit
409         ]
410       },
411       {
412         ObjectId: 2.5.29.15 Criticality=true
413         KeyUsage [
414           Key_CertSign
415           Crl_Sign
416         ]
417       },
418       {
419         ObjectId: 2.5.29.14 Criticality=false
420         SubjectKeyIdentifier [
421         KeyIdentifier [
422         0000: 2C D5 50 41 97 15 8B F0   8F 36 61
    5B 4A FB 6B D9  ,.PA.....6a[J.k.
```

```
423         0010: 99 C9 33 92
                                                ..3.
424         ]
425         ]
426       }
427     ]},
428   "certificate" : {
429     "version"            : "v3",
430     "serial number"      : "00",
431     "signature algorithm": "SHA256withECDSA",
432     "issuer"             : "CN=Hellenic Academic
    and Research Institutions ECC RootCA 2015, O=
    Hellenic Academic and Research Institutions Cert.
    Authority, L=Athens, C=GR",
433     "not before"         : "2015-07-07 18:37:12.
    000 SGT",
434     "not  after"         : "2040-06-30 18:37:12.
    000 SGT",
435     "subject"            : "CN=Hellenic Academic
    and Research Institutions ECC RootCA 2015, O=
    Hellenic Academic and Research Institutions Cert.
    Authority, L=Athens, C=GR",
436     "subject public key" : "EC",
437     "extensions"         : [
438       {
439         ObjectId: 2.5.29.19 Criticality=true
440         BasicConstraints:[
441           CA:true
442           PathLen: no limit
443         ]
444       },
445       {
446         ObjectId: 2.5.29.15 Criticality=true
447         KeyUsage [
448           Key_CertSign
449           Crl_Sign
450         ]
451       },
452       {
453         ObjectId: 2.5.29.14 Criticality=false
454         SubjectKeyIdentifier [
```

```
455         KeyIdentifier [
456         0000: B4 22 0B 82 99 24 01 0E   9C BB E4
    0E FD BF FB 97  ."...$.........
457         0010: 20 93 99 2A
                                                ..*
458         ]
459         ]
460       }
461     ]},
462   "certificate" : {
463     "version"            : "v3",
464     "serial number"      : "00",
465     "signature algorithm": "SHA256withRSA",
466     "issuer"             : "OU=Security
    Communication RootCA2, O="SECOM Trust Systems CO.,
    LTD.", C=JP",
467     "not before"         : "2009-05-29 13:00:39.
    000 SGT",
468     "not  after"         : "2029-05-29 13:00:39.
    000 SGT",
469     "subject"            : "OU=Security
    Communication RootCA2, O="SECOM Trust Systems CO.,
    LTD.", C=JP",
470     "subject public key" : "RSA",
471     "extensions"         : [
472       {
473         ObjectId: 2.5.29.19 Criticality=true
474         BasicConstraints:[
475           CA:true
476           PathLen: no limit
477         ]
478       },
479       {
480         ObjectId: 2.5.29.15 Criticality=true
481         KeyUsage [
482           Key_CertSign
483           Crl_Sign
484         ]
485       },
486       {
487         ObjectId: 2.5.29.14 Criticality=false
```

```
488         SubjectKeyIdentifier [
489         KeyIdentifier [
490         0000: 0A 85 A9 77 65 05 98 7C   40 81 F8
    0F 97 2C 38 F1  ...we...@....,8.
491         0010: 0A EC 3C CF
                                                ..<.
492         ]
493         ]
494       }
495     ]},
496   "certificate" : {
497     "version"            : "v3",
498     "serial number"      : "3CF607A968700EDA8B84",
499     "signature algorithm": "SHA384withECDSA",
500     "issuer"             : "CN=emSign ECC Root CA
     - G3, O=eMudhra Technologies Limited, OU=emSign
    PKI, C=IN",
501     "not before"         : "2018-02-19 02:30:00.
    000 SGT",
502     "not  after"         : "2043-02-19 02:30:00.
    000 SGT",
503     "subject"            : "CN=emSign ECC Root CA
     - G3, O=eMudhra Technologies Limited, OU=emSign
    PKI, C=IN",
504     "subject public key" : "EC",
505     "extensions"         : [
506       {
507         ObjectId: 2.5.29.19 Criticality=true
508         BasicConstraints:[
509           CA:true
510           PathLen: no limit
511         ]
512       },
513       {
514         ObjectId: 2.5.29.15 Criticality=true
515         KeyUsage [
516           Key_CertSign
517           Crl_Sign
518         ]
519       },
520       {
```

```
521         ObjectId: 2.5.29.14 Criticality=false
522         SubjectKeyIdentifier [
523         KeyIdentifier [
524         0000: 7C 5D 02 84 13 D4 CC 8A   9B 81 CE
    17 1C 2E 29 1E  .]..........).
525         0010: 9C 48 63 42
                                           .HcB
526         ]
527         ]
528       }
529     ]},
530   "certificate" : {
531     "version"            : "v3",
532     "serial number"      : "
    15C8BD65475CAFB897005EE406D2BC9D",
533     "signature algorithm": "SHA1withRSA",
534     "issuer"             : "OU=ePKI Root
    Certification Authority, O="Chunghwa Telecom Co.,
    Ltd.", C=TW",
535     "not before"         : "2004-12-20 10:31:27.
    000 SGT",
536     "not  after"         : "2034-12-20 10:31:27.
    000 SGT",
537     "subject"            : "OU=ePKI Root
    Certification Authority, O="Chunghwa Telecom Co.,
    Ltd.", C=TW",
538     "subject public key" : "RSA",
539     "extensions"         : [
540       {
541         ObjectId: 2.23.42.7.0 Criticality=false
542       },
543       {
544         ObjectId: 2.5.29.19 Criticality=false
545         BasicConstraints:[
546           CA:true
547           PathLen: no limit
548         ]
549       },
550       {
551         ObjectId: 2.5.29.14 Criticality=false
552         SubjectKeyIdentifier [
```

```
553         KeyIdentifier [
554         0000: 1E 0C F7 B6 67 F2 E1 92   26 09 45
    C0 55 39 2E 77  ....g...&.E.U9.w
555         0010: 3F 42 4A A2
                                            ?BJ.
556         ]
557         ]
558       }
559     ]},
560   "certificate" : {
561     "version"            : "v3",
562     "serial number"      : "7777062726A9B17C",
563     "signature algorithm": "SHA256withRSA",
564     "issuer"             : "CN=AffirmTrust
    Commercial, O=AffirmTrust, C=US",
565     "not before"         : "2010-01-29 22:06:06.
    000 SGT",
566     "not  after"         : "2030-12-31 22:06:06.
    000 SGT",
567     "subject"            : "CN=AffirmTrust
    Commercial, O=AffirmTrust, C=US",
568     "subject public key" : "RSA",
569     "extensions"         : [
570       {
571         ObjectId: 2.5.29.19 Criticality=true
572         BasicConstraints:[
573           CA:true
574           PathLen: no limit
575         ]
576       },
577       {
578         ObjectId: 2.5.29.15 Criticality=true
579         KeyUsage [
580           Key_CertSign
581           Crl_Sign
582         ]
583       },
584       {
585         ObjectId: 2.5.29.14 Criticality=false
586         SubjectKeyIdentifier [
587         KeyIdentifier [
```

```
588         0000: 9D 93 C6 53 8B 5E CA AF   3F 9F 1E
    0F E5 99 95 BC  ...S.^..?.......
589         0010: 24 F6 94 8F
                                            $...
590         ]
591         ]
592       }
593     ]},
594   "certificate" : {
595     "version"            : "v3",
596     "serial number"      : "0444C0",
597     "signature algorithm": "SHA1withRSA",
598     "issuer"             : "CN=Certum Trusted
    Network CA, OU=Certum Certification Authority, O=
    Unizeto Technologies S.A., C=PL",
599     "not before"         : "2008-10-22 20:07:37.
    000 SGT",
600     "not  after"         : "2029-12-31 20:07:37.
    000 SGT",
601     "subject"            : "CN=Certum Trusted
    Network CA, OU=Certum Certification Authority, O=
    Unizeto Technologies S.A., C=PL",
602     "subject public key" : "RSA",
603     "extensions"         : [
604       {
605         ObjectId: 2.5.29.19 Criticality=true
606         BasicConstraints:[
607           CA:true
608           PathLen: no limit
609         ]
610       },
611       {
612         ObjectId: 2.5.29.15 Criticality=true
613         KeyUsage [
614           Key_CertSign
615           Crl_Sign
616         ]
617       },
618       {
619         ObjectId: 2.5.29.14 Criticality=false
620         SubjectKeyIdentifier [
```

```
621         KeyIdentifier [
622         0000: 08 76 CD CB 07 FF 24 F6   C5 CD ED
    BB 90 BC E2 84  .v....$.........
623         0010: 37 46 75 F7
                                            7Fu.
624         ]
625         ]
626       }
627     ]},
628   "certificate" : {
629     "version"            : "v3",
630     "serial number"      : "
    50946CEC18EAD59C4DD597EF758FA0AD",
631     "signature algorithm": "SHA1withRSA",
632     "issuer"             : "CN=XRamp Global
    Certification Authority, O=XRamp Security Services
     Inc, OU=www.xrampsecurity.com, C=US",
633     "not before"         : "2004-11-02 01:14:04.
    000 SGT",
634     "not  after"         : "2035-01-01 13:37:19.
    000 SGT",
635     "subject"            : "CN=XRamp Global
    Certification Authority, O=XRamp Security Services
     Inc, OU=www.xrampsecurity.com, C=US",
636     "subject public key" : "RSA",
637     "extensions"         : [
638       {
639         ObjectId: 1.3.6.1.4.1.311.20.2 Criticality
    =false
640       },
641       {
642         ObjectId: 1.3.6.1.4.1.311.21.1 Criticality
    =false
643       },
644       {
645         ObjectId: 2.5.29.19 Criticality=true
646         BasicConstraints:[
647           CA:true
648           PathLen: no limit
649         ]
650       },
```

```
651       {
652         ObjectId: 2.5.29.31 Criticality=false
653         CRLDistributionPoints [
654           [DistributionPoint:
655              [URIName: http://crl.xrampsecurity.
    com/XGCA.crl]
656         ]]
657       },
658       {
659         ObjectId: 2.5.29.15 Criticality=false
660         KeyUsage [
661           DigitalSignature
662           Key_CertSign
663           Crl_Sign
664         ]
665       },
666       {
667         ObjectId: 2.5.29.14 Criticality=false
668         SubjectKeyIdentifier [
669         KeyIdentifier [
670         0000: C6 4F A2 3D 06 63 84 09   9C CE 62
    E4 04 AC 8D 5C  .O.=.c....b....\
671         0010: B5 E9 B6 1B
                                                ....
672         ]
673         ]
674       }
675     ]},
676   "certificate" : {
677     "version"            : "v3",
678     "serial number"      : "31F5E4620C6C58EDD6D8",
679     "signature algorithm": "SHA256withRSA",
680     "issuer"             : "CN=emSign Root CA - G1
    , O=eMudhra Technologies Limited, OU=emSign PKI, C
    =IN",
681     "not before"         : "2018-02-19 02:30:00.
    000 SGT",
682     "not  after"         : "2043-02-19 02:30:00.
    000 SGT",
683     "subject"            : "CN=emSign Root CA - G1
    , O=eMudhra Technologies Limited, OU=emSign PKI, C
```

```
683 =IN",
684     "subject public key" : "RSA",
685     "extensions"         : [
686       {
687         ObjectId: 2.5.29.19 Criticality=true
688         BasicConstraints:[
689           CA:true
690           PathLen: no limit
691         ]
692       },
693       {
694         ObjectId: 2.5.29.15 Criticality=true
695         KeyUsage [
696           Key_CertSign
697           Crl_Sign
698         ]
699       },
700       {
701         ObjectId: 2.5.29.14 Criticality=false
702         SubjectKeyIdentifier [
703         KeyIdentifier [
704         0000: FB EF 0D 86 9E B0 E3 DD   A9 B9 F1
    21 17 7F 3E FC  ...........!..>.
705         0010: F0 77 2B 1A
                                                .w+.
706         ]
707         ]
708       }
709     ]},
710   "certificate" : {
711     "version"            : "v3",
712     "serial number"      : "
    00D9B5437FAFA9390F000000005565AD58",
713     "signature algorithm": "SHA256withRSA",
714     "issuer"             : "CN=Entrust Root
    Certification Authority - G4, OU="(c) 2015 Entrust
    , Inc. - for authorized use only", OU=See www.
    entrust.net/legal-terms, O="Entrust, Inc.", C=US",
715     "not before"         : "2015-05-27 19:11:16.
    000 SGT",
716     "not  after"         : "2037-12-27 19:41:16.
```

```
716 000 SGT",
717     "subject"            : "CN=Entrust Root
    Certification Authority - G4, OU="(c) 2015 Entrust
    , Inc. - for authorized use only", OU=See www.
    entrust.net/legal-terms, O="Entrust, Inc.", C=US",
718     "subject public key" : "RSA",
719     "extensions"         : [
720       {
721         ObjectId: 2.5.29.19 Criticality=true
722         BasicConstraints:[
723           CA:true
724           PathLen: no limit
725         ]
726       },
727       {
728         ObjectId: 2.5.29.15 Criticality=true
729         KeyUsage [
730           Key_CertSign
731           Crl_Sign
732         ]
733       },
734       {
735         ObjectId: 2.5.29.14 Criticality=false
736         SubjectKeyIdentifier [
737         KeyIdentifier [
738         0000: 9F 38 C4 56 23 C3 39 E8   A0 71 6C
    E8 54 4C E4 E8  .8.V#.9..ql.TL..
739         0010: 3A B1 BF 67
                                            :..g
740         ]
741         ]
742       }
743     ]},
744   "certificate" : {
745     "version"            : "v3",
746     "serial number"      : "
    3CB2F4480A00E2FEEB243B5E603EC36B",
747     "signature algorithm": "SHA384withECDSA",
748     "issuer"             : "CN=GeoTrust Primary
    Certification Authority - G2, OU=(c) 2007 GeoTrust
     Inc. - For authorized use only, O=GeoTrust Inc.,
```

```
748 C=US",
749     "not before"         : "2007-11-05 08:00:00.
    000 SGT",
750     "not  after"         : "2038-01-19 07:59:59.
    000 SGT",
751     "subject"            : "CN=GeoTrust Primary
    Certification Authority - G2, OU=(c) 2007 GeoTrust
     Inc. - For authorized use only, O=GeoTrust Inc.,
    C=US",
752     "subject public key" : "EC",
753     "extensions"         : [
754       {
755         ObjectId: 2.5.29.19 Criticality=true
756         BasicConstraints:[
757           CA:true
758           PathLen: no limit
759         ]
760       },
761       {
762         ObjectId: 2.5.29.15 Criticality=true
763         KeyUsage [
764           Key_CertSign
765           Crl_Sign
766         ]
767       },
768       {
769         ObjectId: 2.5.29.14 Criticality=false
770         SubjectKeyIdentifier [
771         KeyIdentifier [
772         0000: 15 5F 35 57 51 55 FB 25   B2 AD 03
    69 FC 01 A3 FA  ._5WQU.%...i....
773         0010: BE 11 55 D5
                                                ..U.
774         ]
775         ]
776       }
777     ]},
778   "certificate" : {
779     "version"            : "v3",
780     "serial number"      : "
    01675F27D6FE7AE3E4ACBE095B059E",
```

```
781     "signature algorithm": "SHA256withRSA",
782     "issuer"             : "CN=Telia Root CA v2, O
    =Telia Finland Oyj, C=FI",
783     "not before"         : "2018-11-29 19:55:54.
    000 SGT",
784     "not  after"         : "2043-11-29 19:55:54.
    000 SGT",
785     "subject"            : "CN=Telia Root CA v2, O
    =Telia Finland Oyj, C=FI",
786     "subject public key" : "RSA",
787     "extensions"         : [
788       {
789         ObjectId: 2.5.29.35 Criticality=false
790         AuthorityKeyIdentifier [
791         KeyIdentifier [
792         0000: 72 AC E4 33 79 AA 45 87   F6 FD AC
    1D 9E D6 C7 2F  r..3y.E......../
793         0010: 86 D8 24 39
                                            ..$9
794         ]
795         ]
796       },
797       {
798         ObjectId: 2.5.29.19 Criticality=true
799         BasicConstraints:[
800           CA:true
801           PathLen: no limit
802         ]
803       },
804       {
805         ObjectId: 2.5.29.15 Criticality=true
806         KeyUsage [
807           Key_CertSign
808           Crl_Sign
809         ]
810       },
811       {
812         ObjectId: 2.5.29.14 Criticality=false
813         SubjectKeyIdentifier [
814         KeyIdentifier [
815         0000: 72 AC E4 33 79 AA 45 87   F6 FD AC
```

```
815 1D 9E D6 C7 2F  r..3y.E......./
816         0010: 86 D8 24 39
                                                ..$9
817         ]
818         ]
819       }
820     ]},
821   "certificate" : {
822     "version"            : "v3",
823     "serial number"      : "
    1F47AFAA62007050544C019E9B63992A",
824     "signature algorithm": "SHA384withECDSA",
825     "issuer"             : "CN=COMODO ECC
    Certification Authority, O=COMODO CA Limited, L=
    Salford, ST=Greater Manchester, C=GB",
826     "not before"         : "2008-03-06 08:00:00.
    000 SGT",
827     "not  after"         : "2038-01-19 07:59:59.
    000 SGT",
828     "subject"            : "CN=COMODO ECC
    Certification Authority, O=COMODO CA Limited, L=
    Salford, ST=Greater Manchester, C=GB",
829     "subject public key" : "EC",
830     "extensions"         : [
831       {
832         ObjectId: 2.5.29.19 Criticality=true
833         BasicConstraints:[
834           CA:true
835           PathLen: no limit
836         ]
837       },
838       {
839         ObjectId: 2.5.29.15 Criticality=true
840         KeyUsage [
841           Key_CertSign
842           Crl_Sign
843         ]
844       },
845       {
846         ObjectId: 2.5.29.14 Criticality=false
847         SubjectKeyIdentifier [
```

```
848         KeyIdentifier [
849         0000: 75 71 A7 19 48 19 BC 9D   9D EA 41
    47 DF 94 C4 48  uq..H.....AG...H
850         0010: 77 99 D3 79
                                            w..y
851         ]
852         ]
853       }
854     ]},
855   "certificate" : {
856     "version"            : "v3",
857     "serial number"      : "
    7E00DBB956CF559684CEF156AE142A4FB2FF7503",
858     "signature algorithm": "SHA256withRSA",
859     "issuer"             : "CN=localhost, O=My
    Company, L=San Francisco, ST=California, C=US",
860     "not before"         : "2024-10-30 13:50:49.
    000 SGT",
861     "not  after"         : "2025-10-30 13:50:49.
    000 SGT",
862     "subject"            : "CN=localhost, O=My
    Company, L=San Francisco, ST=California, C=US",
863     "subject public key" : "RSA",
864     "extensions"         : [
865       {
866         ObjectId: 2.5.29.17 Criticality=false
867         SubjectAlternativeName [
868           DNSName: localhost
869         ]
870       },
871       {
872         ObjectId: 2.5.29.14 Criticality=false
873         SubjectKeyIdentifier [
874         KeyIdentifier [
875         0000: 2E AD 8E 81 CE A8 EF 40   6C C3 08
    A3 95 20 11 E2  .......@l.... ..
876         0010: F0 21 68 A3
                                            .!h.
877         ]
878         ]
879       }
```

```
880     ]},
881   "certificate" : {
882     "version"            : "v3",
883     "serial number"      : "
    008210CFB0D240E3594463E0BB63828B00",
884     "signature algorithm": "SHA256withRSA",
885     "issuer"             : "CN=ISRG Root X1, O=
    Internet Security Research Group, C=US",
886     "not before"         : "2015-06-04 19:04:38.
    000 SGT",
887     "not  after"         : "2035-06-04 19:04:38.
    000 SGT",
888     "subject"            : "CN=ISRG Root X1, O=
    Internet Security Research Group, C=US",
889     "subject public key" : "RSA",
890     "extensions"         : [
891       {
892         ObjectId: 2.5.29.19 Criticality=true
893         BasicConstraints:[
894           CA:true
895           PathLen: no limit
896         ]
897       },
898       {
899         ObjectId: 2.5.29.15 Criticality=true
900         KeyUsage [
901           Key_CertSign
902           Crl_Sign
903         ]
904       },
905       {
906         ObjectId: 2.5.29.14 Criticality=false
907         SubjectKeyIdentifier [
908         KeyIdentifier [
909         0000: 79 B4 59 E6 7B B6 E5 E4   01 73 80
    08 88 C8 1A 58  y.Y......s.....X
910         0010: F6 E9 9B 6E
                                                ...n
911         ]
912         ]
913       }
```

```
914     ]},
915   "certificate" : {
916     "version"            : "v3",
917     "serial number"      : "
    02AC5C266A0B409B8F0B79F2AE462577",
918     "signature algorithm": "SHA1withRSA",
919     "issuer"             : "CN=DigiCert High
    Assurance EV Root CA, OU=www.digicert.com, O=
    DigiCert Inc, C=US",
920     "not before"         : "2006-11-10 08:00:00.
    000 SGT",
921     "not  after"         : "2031-11-10 08:00:00.
    000 SGT",
922     "subject"            : "CN=DigiCert High
    Assurance EV Root CA, OU=www.digicert.com, O=
    DigiCert Inc, C=US",
923     "subject public key" : "RSA",
924     "extensions"         : [
925       {
926         ObjectId: 2.5.29.35 Criticality=false
927         AuthorityKeyIdentifier [
928         KeyIdentifier [
929         0000: B1 3E C3 69 03 F8 BF 47   01 D4 98
    26 1A 08 02 EF  .>.i...G...&....
930         0010: 63 64 2B C3
                                            cd+.
931         ]
932         ]
933       },
934       {
935         ObjectId: 2.5.29.19 Criticality=true
936         BasicConstraints:[
937           CA:true
938           PathLen: no limit
939         ]
940       },
941       {
942         ObjectId: 2.5.29.15 Criticality=true
943         KeyUsage [
944           DigitalSignature
945           Key_CertSign
```

```
946           Crl_Sign
947         ]
948       },
949       {
950         ObjectId: 2.5.29.14 Criticality=false
951         SubjectKeyIdentifier [
952         KeyIdentifier [
953         0000: B1 3E C3 69 03 F8 BF 47   01 D4 98
    26 1A 08 02 EF  .>.i...G...&....
954         0010: 63 64 2B C3
                                            cd+.
955         ]
956         ]
957       }
958     ]},
959   "certificate" : {
960     "version"            : "v3",
961     "serial number"      : "01",
962     "signature algorithm": "SHA1withRSA",
963     "issuer"             : "CN=GeoTrust Universal
    CA, O=GeoTrust Inc., C=US",
964     "not before"         : "2004-03-04 13:00:00.
    000 SGT",
965     "not  after"         : "2029-03-04 13:00:00.
    000 SGT",
966     "subject"            : "CN=GeoTrust Universal
    CA, O=GeoTrust Inc., C=US",
967     "subject public key" : "RSA",
968     "extensions"         : [
969       {
970         ObjectId: 2.5.29.35 Criticality=false
971         AuthorityKeyIdentifier [
972         KeyIdentifier [
973         0000: DA BB 2E AA B0 0C B8 88   26 51 74
    5C 6D 03 D3 C0  ........&Qt\m...
974         0010: D8 8F 7A D6
                                            ..z.
975         ]
976         ]
977       },
978       {
```

```
 979         ObjectId: 2.5.29.19 Criticality=true
 980         BasicConstraints:[
 981           CA:true
 982           PathLen: no limit
 983         ]
 984       },
 985       {
 986         ObjectId: 2.5.29.15 Criticality=true
 987         KeyUsage [
 988           DigitalSignature
 989           Key_CertSign
 990           Crl_Sign
 991         ]
 992       },
 993       {
 994         ObjectId: 2.5.29.14 Criticality=false
 995         SubjectKeyIdentifier [
 996         KeyIdentifier [
 997         0000: DA BB 2E AA B0 0C B8 88   26 51 74
     5C 6D 03 D3 C0  ........&Qt\m...
 998         0010: D8 8F 7A D6
                                                ..z.
 999         ]
1000         ]
1001       }
1002     ]},
1003   "certificate" : {
1004     "version"            : "v3",
1005     "serial number"      : "
     04000000000121585308A2",
1006     "signature algorithm": "SHA256withRSA",
1007     "issuer"             : "CN=GlobalSign, O=
     GlobalSign, OU=GlobalSign Root CA - R3",
1008     "not before"         : "2009-03-18 18:00:00.
     000 SGT",
1009     "not  after"         : "2029-03-18 18:00:00.
     000 SGT",
1010     "subject"            : "CN=GlobalSign, O=
     GlobalSign, OU=GlobalSign Root CA - R3",
1011     "subject public key" : "RSA",
1012     "extensions"         : [
```

```
1013        {
1014          ObjectId: 2.5.29.19 Criticality=true
1015          BasicConstraints:[
1016            CA:true
1017            PathLen: no limit
1018          ]
1019        },
1020        {
1021          ObjectId: 2.5.29.15 Criticality=true
1022          KeyUsage [
1023            Key_CertSign
1024            Crl_Sign
1025          ]
1026        },
1027        {
1028          ObjectId: 2.5.29.14 Criticality=false
1029          SubjectKeyIdentifier [
1030          KeyIdentifier [
1031          0000: 8F F0 4B 7F A8 2E 45 24   AE 4D 50
     FA 63 9A 8B DE  ..K...E$.MP.c...
1032          0010: E2 DD 1B BC
                                              ....
1033          ]
1034          ]
1035        }
1036      ]},
1037    "certificate" : {
1038      "version"            : "v3",
1039      "serial number"      : "020000B9",
1040      "signature algorithm": "SHA1withRSA",
1041      "issuer"             : "CN=Baltimore
     CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
     ",
1042      "not before"         : "2000-05-13 02:46:00.
     000 SGT",
1043      "not  after"         : "2025-05-13 07:59:00.
     000 SGT",
1044      "subject"            : "CN=Baltimore
     CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
     ",
1045      "subject public key" : "RSA",
```

```
1046     "extensions"          : [
1047       {
1048         ObjectId: 2.5.29.19 Criticality=true
1049         BasicConstraints:[
1050           CA:true
1051           PathLen:3
1052         ]
1053       },
1054       {
1055         ObjectId: 2.5.29.15 Criticality=true
1056         KeyUsage [
1057           Key_CertSign
1058           Crl_Sign
1059         ]
1060       },
1061       {
1062         ObjectId: 2.5.29.14 Criticality=false
1063         SubjectKeyIdentifier [
1064         KeyIdentifier [
1065         0000: E5 9D 59 30 82 47 58 CC   AC FA 08
     54 36 86 7B 3A  ..Y0.GX....T6..:
1066         0010: B5 04 4D F0
                                                ..M.
1067         ]
1068         ]
1069       }
1070     ]},
1071   "certificate" : {
1072     "version"             : "v3",
1073     "serial number"       : "01",
1074     "signature algorithm": "SHA1withRSA",
1075     "issuer"              : "CN=AAA Certificate
     Services, O=Comodo CA Limited, L=Salford, ST=
     Greater Manchester, C=GB",
1076     "not before"          : "2004-01-01 08:00:00.
     000 SGT",
1077     "not  after"          : "2029-01-01 07:59:59.
     000 SGT",
1078     "subject"             : "CN=AAA Certificate
     Services, O=Comodo CA Limited, L=Salford, ST=
     Greater Manchester, C=GB",
```

```
    "subject public key" : "RSA",
    "extensions"         : [
      {
        ObjectId: 2.5.29.19 Criticality=true
        BasicConstraints:[
          CA:true
          PathLen: no limit
        ]
      },
      {
        ObjectId: 2.5.29.31 Criticality=false
        CRLDistributionPoints [
          [DistributionPoint:
             [URIName: http://crl.comodoca.com/
    AAACertificateServices.crl]
        , DistributionPoint:
             [URIName: http://crl.comodo.net/
    AAACertificateServices.crl]
        ]]
      },
      {
        ObjectId: 2.5.29.15 Criticality=true
        KeyUsage [
          Key_CertSign
          Crl_Sign
        ]
      },
      {
        ObjectId: 2.5.29.14 Criticality=false
        SubjectKeyIdentifier [
        KeyIdentifier [
        0000: A0 11 0A 23 3E 96 F1 07   EC E2 AF
    29 EF 82 A5 7F  ...#>......)....
        0010: D0 30 A4 B4
                                            .0..
        ]
        ]
      }
    ]},
  "certificate" : {
    "version"            : "v3",
```

```
1116     "serial number"      : "00",
1117     "signature algorithm": "SHA1withRSA",
1118     "issuer"             : "OU=Starfield Class 2
     Certification Authority, O="Starfield
     Technologies, Inc.", C=US",
1119     "not before"         : "2004-06-30 01:39:16.
     000 SGT",
1120     "not  after"         : "2034-06-30 01:39:16.
     000 SGT",
1121     "subject"            : "OU=Starfield Class 2
     Certification Authority, O="Starfield
     Technologies, Inc.", C=US",
1122     "subject public key" : "RSA",
1123     "extensions"         : [
1124       {
1125         ObjectId: 2.5.29.35 Criticality=false
1126         AuthorityKeyIdentifier [
1127         KeyIdentifier [
1128         0000: BF 5F B7 D1 CE DD 1F 86   F4 5B 55
     AC DC D7 10 C2  ._.......[U.....
1129         0010: 0E A9 88 E7
                                                ....
1130         ]
1131         [OU=Starfield Class 2 Certification
     Authority, O="Starfield Technologies, Inc.", C=US
     ]
1132         SerialNumber: [    00]
1133         ]
1134       },
1135       {
1136         ObjectId: 2.5.29.19 Criticality=false
1137         BasicConstraints:[
1138           CA:true
1139           PathLen: no limit
1140         ]
1141       },
1142       {
1143         ObjectId: 2.5.29.14 Criticality=false
1144         SubjectKeyIdentifier [
1145         KeyIdentifier [
1146         0000: BF 5F B7 D1 CE DD 1F 86   F4 5B 55
```

```
1146 AC DC D7 10 C2  ._.......[U.....
1147         0010: 0E A9 88 E7
                                                ....
1148         ]
1149         ]
1150       }
1151     ]},
1152   "certificate" : {
1153     "version"            : "v3",
1154     "serial number"      : "00",
1155     "signature algorithm": "SHA1withRSA",
1156     "issuer"             : "CN=Chambers of
     Commerce Root, OU=http://www.chambersign.org, O=
     AC Camerfirma SA CIF A82743287, C=EU",
1157     "not before"         : "2003-10-01 24:13:43.
     000 SGT",
1158     "not  after"         : "2037-10-01 24:13:44.
     000 SGT",
1159     "subject"            : "CN=Chambers of
     Commerce Root, OU=http://www.chambersign.org, O=
     AC Camerfirma SA CIF A82743287, C=EU",
1160     "subject public key" : "RSA",
1161     "extensions"         : [
1162       {
1163         ObjectId: 2.5.29.19 Criticality=true
1164         BasicConstraints:[
1165           CA:true
1166           PathLen:12
1167         ]
1168       },
1169       {
1170         ObjectId: 2.5.29.31 Criticality=false
1171         CRLDistributionPoints [
1172           [DistributionPoint:
1173              [URIName: http://crl.chambersign.org
     /chambersroot.crl]
1174         ]]
1175       },
1176       {
1177         ObjectId: 2.5.29.32 Criticality=false
1178         CertificatePolicies [
```

```
1179           [CertificatePolicyId: [1.3.6.1.4.1.
     17326.10.3.1]
1180         [PolicyQualifierInfo: [
1181           qualifierID: 1.3.6.1.5.5.7.2.1
1182           qualifier: 0000: 16 30 68 74 74 70 3A
     2F   2F 63 70 73 2E 63 68 61  .0http://cps.cha
1183         0010: 6D 62 65 72 73 69 67 6E   2E 6F 72
     67 2F 63 70 73  mbersign.org/cps
1184         0020: 2F 63 68 61 6D 62 65 72   73 72 6F
     6F 74 2E 68 74  /chambersroot.ht
1185         0030: 6D 6C
                                                    ml
1186
1187         ]]  ]
1188         ]
1189       },
1190       {
1191         ObjectId: 2.5.29.18 Criticality=false
1192         IssuerAlternativeName [
1193           RFC822Name: chambersroot@chambersign.
     org
1194         ]
1195       },
1196       {
1197         ObjectId: 2.5.29.15 Criticality=true
1198         KeyUsage [
1199           Key_CertSign
1200           Crl_Sign
1201         ]
1202       },
1203       {
1204         ObjectId: 2.16.840.1.113730.1.1
     Criticality=false
1205         NetscapeCertType [
1206            SSL CA
1207            S/MIME CA
1208            Object Signing CA]
1209       },
1210       {
1211         ObjectId: 2.5.29.17 Criticality=false
1212         SubjectAlternativeName [
```

```
1213           RFC822Name: chambersroot@chambersign.
     org
1214         ]
1215       },
1216       {
1217         ObjectId: 2.5.29.14 Criticality=false
1218         SubjectKeyIdentifier [
1219         KeyIdentifier [
1220         0000: E3 94 F5 B1 4D E9 DB A1   29 5B 57
     8B 4D 76 06 76  ....M...)[W.Mv.v
1221         0010: E1 D1 A2 8A
                                                ....
1222         ]
1223         ]
1224       }
1225     ]},
1226   "certificate" : {
1227     "version"            : "v1",
1228     "serial number"      : "
     009B7E0649A33E62B9D5EE90487129EF57",
1229     "signature algorithm": "SHA1withRSA",
1230     "issuer"             : "CN=VeriSign Class 3
     Public Primary Certification Authority - G3, OU
     ="(c) 1999 VeriSign, Inc. - For authorized use
     only", OU=VeriSign Trust Network, O="VeriSign,
     Inc.", C=US",
1231     "not before"         : "1999-10-01 08:00:00.
     000 SGT",
1232     "not  after"         : "2036-07-17 07:59:59.
     000 SGT",
1233     "subject"            : "CN=VeriSign Class 3
     Public Primary Certification Authority - G3, OU
     ="(c) 1999 VeriSign, Inc. - For authorized use
     only", OU=VeriSign Trust Network, O="VeriSign,
     Inc.", C=US",
1234     "subject public key" : "RSA"},
1235   "certificate" : {
1236     "version"            : "v3",
1237     "serial number"      : "
     040000000001154B5AC394",
1238     "signature algorithm": "SHA1withRSA",
```

```
1239     "issuer"              : "CN=GlobalSign Root CA
     , OU=Root CA, O=GlobalSign nv-sa, C=BE",
1240     "not before"          : "1998-09-01 20:00:00.
     000 SGT",
1241     "not  after"          : "2028-01-28 20:00:00.
     000 SGT",
1242     "subject"             : "CN=GlobalSign Root CA
     , OU=Root CA, O=GlobalSign nv-sa, C=BE",
1243     "subject public key" : "RSA",
1244     "extensions"          : [
1245       {
1246         ObjectId: 2.5.29.19 Criticality=true
1247         BasicConstraints:[
1248           CA:true
1249           PathLen: no limit
1250         ]
1251       },
1252       {
1253         ObjectId: 2.5.29.15 Criticality=true
1254         KeyUsage [
1255           Key_CertSign
1256           Crl_Sign
1257         ]
1258       },
1259       {
1260         ObjectId: 2.5.29.14 Criticality=false
1261         SubjectKeyIdentifier [
1262         KeyIdentifier [
1263         0000: 60 7B 66 1A 45 0D 97 CA   89 50 2F
     7D 04 CD 34 A8  `.f.E....P/...4.
1264         0010: FF FC FD 4B
                                             ...K
1265         ]
1266         ]
1267       }
1268     ]},
1269   "certificate" : {
1270     "version"             : "v3",
1271     "serial number"       : "
     44BE0C8B500024B411D3362DE0B35F1B",
1272     "signature algorithm": "SHA1withRSA",
```

```
1273     "issuer"             : "CN=UTN-USERFirst-
     Object, OU=http://www.usertrust.com, O=The
     USERTRUST Network, L=Salt Lake City, ST=UT, C=US
     ",
1274     "not before"         : "1999-07-10 02:31:20.
     000 SGT",
1275     "not  after"         : "2019-07-10 02:40:36.
     000 SGT",
1276     "subject"            : "CN=UTN-USERFirst-
     Object, OU=http://www.usertrust.com, O=The
     USERTRUST Network, L=Salt Lake City, ST=UT, C=US
     ",
1277     "subject public key" : "RSA",
1278     "extensions"         : [
1279       {
1280         ObjectId: 2.5.29.19 Criticality=true
1281         BasicConstraints:[
1282           CA:true
1283           PathLen: no limit
1284         ]
1285       },
1286       {
1287         ObjectId: 2.5.29.31 Criticality=false
1288         CRLDistributionPoints [
1289           [DistributionPoint:
1290              [URIName: http://crl.usertrust.com/
     UTN-USERFirst-Object.crl]
1291         ]]
1292       },
1293       {
1294         ObjectId: 2.5.29.37 Criticality=false
1295         ExtendedKeyUsages [
1296           codeSigning
1297           timeStamping
1298           1.3.6.1.4.1.311.10.3.4
1299         ]
1300       },
1301       {
1302         ObjectId: 2.5.29.15 Criticality=false
1303         KeyUsage [
1304           DigitalSignature
```

```
1305           Non_repudiation
1306           Key_CertSign
1307           Crl_Sign
1308         ]
1309       },
1310       {
1311         ObjectId: 2.5.29.14 Criticality=false
1312         SubjectKeyIdentifier [
1313         KeyIdentifier [
1314         0000: DA ED 64 74 14 9C 14 3C   AB DD 99
     A9 BD 5B 28 4D  ..dt...<.....[(M
1315         0010: 8B 3C C9 D8
                                            .<..
1316         ]
1317         ]
1318       }
1319     ]},
1320   "certificate" : {
1321     "version"            : "v3",
1322     "serial number"      : "7C4F04391CD4992D",
1323     "signature algorithm": "SHA1withRSA",
1324     "issuer"             : "CN=AffirmTrust
     Networking, O=AffirmTrust, C=US",
1325     "not before"         : "2010-01-29 22:08:24.
     000 SGT",
1326     "not  after"         : "2030-12-31 22:08:24.
     000 SGT",
1327     "subject"            : "CN=AffirmTrust
     Networking, O=AffirmTrust, C=US",
1328     "subject public key" : "RSA",
1329     "extensions"         : [
1330       {
1331         ObjectId: 2.5.29.19 Criticality=true
1332         BasicConstraints:[
1333           CA:true
1334           PathLen: no limit
1335         ]
1336       },
1337       {
1338         ObjectId: 2.5.29.15 Criticality=true
1339         KeyUsage [
```

```
1340           Key_CertSign
1341           Crl_Sign
1342         ]
1343       },
1344       {
1345         ObjectId: 2.5.29.14 Criticality=false
1346         SubjectKeyIdentifier [
1347         KeyIdentifier [
1348         0000: 07 1F D2 E7 9C DA C2 6E   A2 40 B4
     B0 7A 50 10 50  .......n.@..zP.P
1349         0010: 74 C4 C8 BD
                                            t...
1350         ]
1351         ]
1352       }
1353     ]},
1354   "certificate" : {
1355     "version"            : "v3",
1356     "serial number"      : "0CBE",
1357     "signature algorithm": "SHA256withRSA",
1358     "issuer"             : "CN=TWCA Global Root
     CA, OU=Root CA, O=TAIWAN-CA, C=TW",
1359     "not before"         : "2012-06-27 14:28:33.
     000 SGT",
1360     "not  after"         : "2030-12-31 23:59:59.
     000 SGT",
1361     "subject"            : "CN=TWCA Global Root
     CA, OU=Root CA, O=TAIWAN-CA, C=TW",
1362     "subject public key" : "RSA",
1363     "extensions"         : [
1364       {
1365         ObjectId: 2.5.29.19 Criticality=true
1366         BasicConstraints:[
1367           CA:true
1368           PathLen: no limit
1369         ]
1370       },
1371       {
1372         ObjectId: 2.5.29.15 Criticality=true
1373         KeyUsage [
1374           Key_CertSign
```

```
1375           Crl_Sign
1376         ]
1377       }
1378     ]},
1379   "certificate" : {
1380     "version"            : "v3",
1381     "serial number"      : "6D8C1446B1A60AEE",
1382     "signature algorithm": "SHA384withRSA",
1383     "issuer"             : "CN=AffirmTrust
     Premium, O=AffirmTrust, C=US",
1384     "not before"         : "2010-01-29 22:10:36.
     000 SGT",
1385     "not  after"         : "2040-12-31 22:10:36.
     000 SGT",
1386     "subject"            : "CN=AffirmTrust
     Premium, O=AffirmTrust, C=US",
1387     "subject public key" : "RSA",
1388     "extensions"         : [
1389       {
1390         ObjectId: 2.5.29.19 Criticality=true
1391         BasicConstraints:[
1392           CA:true
1393           PathLen: no limit
1394         ]
1395       },
1396       {
1397         ObjectId: 2.5.29.15 Criticality=true
1398         KeyUsage [
1399           Key_CertSign
1400           Crl_Sign
1401         ]
1402       },
1403       {
1404         ObjectId: 2.5.29.14 Criticality=false
1405         SubjectKeyIdentifier [
1406         KeyIdentifier [
1407         0000: 9D C0 67 A6 0C 22 D9 26   F5 45 AB
     A6 65 52 11 27  ..g..".&.E..eR.'
1408         0010: D8 45 AC 63
                                            .E.c
1409         ]
```

```
1410         ]
1411       }
1412     ]},
1413   "certificate" : {
1414     "version"            : "v3",
1415     "serial number"      : "0BB8",
1416     "signature algorithm": "SHA256withRSA",
1417     "issuer"             : "CN=LuxTrust Global
     Root, O=LuxTrust s.a., C=LU",
1418     "not before"         : "2011-03-17 17:51:37.
     000 SGT",
1419     "not  after"         : "2021-03-17 17:51:37.
     000 SGT",
1420     "subject"            : "CN=LuxTrust Global
     Root, O=LuxTrust s.a., C=LU",
1421     "subject public key" : "RSA",
1422     "extensions"         : [
1423       {
1424         ObjectId: 2.5.29.35 Criticality=false
1425         AuthorityKeyIdentifier [
1426         KeyIdentifier [
1427         0000: 17 15 85 89 09 2F 24 87   6F 3F 1D
     1B E4 F2 96 79  ...../$.o?.....y
1428         0010: 83 48 13 CE
                                                .H..
1429         ]
1430         ]
1431       },
1432       {
1433         ObjectId: 2.5.29.19 Criticality=false
1434         BasicConstraints:[
1435           CA:true
1436           PathLen: no limit
1437         ]
1438       },
1439       {
1440         ObjectId: 2.5.29.15 Criticality=true
1441         KeyUsage [
1442           Key_CertSign
1443           Crl_Sign
1444         ]
```

```
1445       },
1446       {
1447         ObjectId: 2.5.29.14 Criticality=false
1448         SubjectKeyIdentifier [
1449         KeyIdentifier [
1450         0000: 17 15 85 89 09 2F 24 87   6F 3F 1D
     1B E4 F2 96 79  ...../$.o?.....y
1451         0010: 83 48 13 CE
                                                .H..
1452         ]
1453         ]
1454       }
1455     ]},
1456   "certificate" : {
1457     "version"            : "v3",
1458     "serial number"      : "
     09E09365ACF7D9C8B93E1C0B042A2EF3",
1459     "signature algorithm": "SHA384withECDSA",
1460     "issuer"             : "CN=DigiCert TLS ECC
     P384 Root G5, O="DigiCert, Inc.", C=US",
1461     "not before"         : "2021-01-15 08:00:00.
     000 SGT",
1462     "not  after"         : "2046-01-15 07:59:59.
     000 SGT",
1463     "subject"            : "CN=DigiCert TLS ECC
     P384 Root G5, O="DigiCert, Inc.", C=US",
1464     "subject public key" : "EC",
1465     "extensions"         : [
1466       {
1467         ObjectId: 2.5.29.19 Criticality=true
1468         BasicConstraints:[
1469           CA:true
1470           PathLen: no limit
1471         ]
1472       },
1473       {
1474         ObjectId: 2.5.29.15 Criticality=true
1475         KeyUsage [
1476           DigitalSignature
1477           Key_CertSign
1478           Crl_Sign
```

```
1479          ]
1480        },
1481        {
1482          ObjectId: 2.5.29.14 Criticality=false
1483          SubjectKeyIdentifier [
1484          KeyIdentifier [
1485          0000: C1 51 45 50 59 AB 3E E7   2C 5A FA
     20 22 12 07 80  .QEPY.>.,Z. "...
1486          0010: 88 7C 11 6A
                                              ...j
1487          ]
1488          ]
1489        }
1490      ]},
1491    "certificate" : {
1492      "version"            : "v3",
1493      "serial number"      : "
     15AC6E9419B2794B41F627A9C3180F1F",
1494      "signature algorithm": "SHA256withRSA",
1495      "issuer"             : "CN=GeoTrust Primary
     Certification Authority - G3, OU=(c) 2008
     GeoTrust Inc. - For authorized use only, O=
     GeoTrust Inc., C=US",
1496      "not before"         : "2008-04-02 08:00:00.
     000 SGT",
1497      "not  after"         : "2037-12-02 07:59:59.
     000 SGT",
1498      "subject"            : "CN=GeoTrust Primary
     Certification Authority - G3, OU=(c) 2008
     GeoTrust Inc. - For authorized use only, O=
     GeoTrust Inc., C=US",
1499      "subject public key" : "RSA",
1500      "extensions"         : [
1501        {
1502          ObjectId: 2.5.29.19 Criticality=true
1503          BasicConstraints:[
1504            CA:true
1505            PathLen: no limit
1506          ]
1507        },
1508        {
```

```
1509         ObjectId: 2.5.29.15 Criticality=true
1510         KeyUsage [
1511           Key_CertSign
1512           Crl_Sign
1513         ]
1514       },
1515       {
1516         ObjectId: 2.5.29.14 Criticality=false
1517         SubjectKeyIdentifier [
1518         KeyIdentifier [
1519         0000: C4 79 CA 8E A1 4E 03 1D   1C DC 6B
     DB 31 5B 94 3E  .y...N....k.1[.>
1520         0010: 3F 30 7F 2D
                                                ?0.-
1521         ]
1522         ]
1523       }
1524     ]},
1525   "certificate" : {
1526     "version"            : "v3",
1527     "serial number"      : "
     0203E5C068EF631A9C72905052",
1528     "signature algorithm": "SHA384withECDSA",
1529     "issuer"             : "CN=GTS Root R4, O=
     Google Trust Services LLC, C=US",
1530     "not before"         : "2016-06-22 08:00:00.
     000 SGT",
1531     "not  after"         : "2036-06-22 08:00:00.
     000 SGT",
1532     "subject"            : "CN=GTS Root R4, O=
     Google Trust Services LLC, C=US",
1533     "subject public key" : "EC",
1534     "extensions"         : [
1535       {
1536         ObjectId: 2.5.29.19 Criticality=true
1537         BasicConstraints:[
1538           CA:true
1539           PathLen: no limit
1540         ]
1541       },
1542       {
```

```
1543         ObjectId: 2.5.29.15 Criticality=true
1544         KeyUsage [
1545           DigitalSignature
1546           Key_CertSign
1547           Crl_Sign
1548         ]
1549       },
1550       {
1551         ObjectId: 2.5.29.14 Criticality=false
1552         SubjectKeyIdentifier [
1553         KeyIdentifier [
1554         0000: 80 4C D6 EB 74 FF 49 36   A3 D5 D8
     FC B5 3E C5 6A  .L..t.I6.....>.j
1555         0010: F0 94 1D 8C
                                                ....
1556         ]
1557         ]
1558       }
1559     ]},
1560   "certificate" : {
1561     "version"            : "v3",
1562     "serial number"      : "
     0A7EA6DF4B449EDA6A24859EE6B815D3167FBBB1",
1563     "signature algorithm": "SHA256withRSA",
1564     "issuer"             : "CN=LuxTrust Global
     Root 2, O=LuxTrust S.A., C=LU",
1565     "not before"         : "2015-03-05 21:21:57.
     000 SGT",
1566     "not  after"         : "2035-03-05 21:21:57.
     000 SGT",
1567     "subject"            : "CN=LuxTrust Global
     Root 2, O=LuxTrust S.A., C=LU",
1568     "subject public key" : "RSA",
1569     "extensions"         : [
1570       {
1571         ObjectId: 2.5.29.35 Criticality=false
1572         AuthorityKeyIdentifier [
1573         KeyIdentifier [
1574         0000: FF 18 28 76 F9 48 05 2C   A1 AE F1
     2B 1B 2B B2 53  ..(v.H.,...+.+.S
1575         0010: F8 4B 7C B3
```

```
1575                                                .K..
1576         ]
1577         ]
1578       },
1579       {
1580         ObjectId: 2.5.29.19 Criticality=true
1581         BasicConstraints:[
1582           CA:true
1583           PathLen: no limit
1584         ]
1585       },
1586       {
1587         ObjectId: 2.5.29.32 Criticality=false
1588         CertificatePolicies [
1589           [CertificatePolicyId: [1.3.171.1.1.1.10
     ]
1590         [PolicyQualifierInfo: [
1591           qualifierID: 1.3.6.1.5.5.7.2.1
1592           qualifier: 0000: 16 1E 68 74 74 70 73
     3A   2F 2F 72 65 70 6F 73 69  ..https://reposi
1593         0010: 74 6F 72 79 2E 6C 75 78   74 72 75
     73 74 2E 6C 75  tory.luxtrust.lu
1594
1595         ]]  ]
1596         ]
1597       },
1598       {
1599         ObjectId: 2.5.29.15 Criticality=true
1600         KeyUsage [
1601           Key_CertSign
1602           Crl_Sign
1603         ]
1604       },
1605       {
1606         ObjectId: 2.5.29.14 Criticality=false
1607         SubjectKeyIdentifier [
1608         KeyIdentifier [
1609         0000: FF 18 28 76 F9 48 05 2C   A1 AE F1
     2B 1B 2B B2 53  ..(v.H.,...+.+.S
1610         0010: F8 4B 7C B3
                                                .K..
```

```
1611          ]
1612          ]
1613        }
1614      ]},
1615    "certificate" : {
1616      "version"            : "v3",
1617      "serial number"      : "00A3DA427EA4B1AEDA",
1618      "signature algorithm": "SHA1withRSA",
1619      "issuer"             : "CN=Chambers of
     Commerce Root - 2008, O=AC Camerfirma S.A.,
     SERIALNUMBER=A82743287, L=Madrid (see current
     address at www.camerfirma.com/address), C=EU",
1620      "not before"         : "2008-08-01 20:29:50.
     000 SGT",
1621      "not  after"         : "2038-07-31 20:29:50.
     000 SGT",
1622      "subject"            : "CN=Chambers of
     Commerce Root - 2008, O=AC Camerfirma S.A.,
     SERIALNUMBER=A82743287, L=Madrid (see current
     address at www.camerfirma.com/address), C=EU",
1623      "subject public key" : "RSA",
1624      "extensions"         : [
1625        {
1626          ObjectId: 2.5.29.35 Criticality=false
1627          AuthorityKeyIdentifier [
1628          KeyIdentifier [
1629          0000: F9 24 AC 0F B2 B5 F8 79   C0 FA 60
     88 1B C4 D9 4D  .$.....y..`....M
1630          0010: 02 9E 17 19
                                              ....
1631          ]
1632          [CN=Chambers of Commerce Root - 2008, O=
     AC Camerfirma S.A., SERIALNUMBER=A82743287, L=
     Madrid (see current address at www.camerfirma.com
     /address), C=EU]
1633          SerialNumber: [    a3da427e a4b1aeda]
1634          ]
1635        },
1636        {
1637          ObjectId: 2.5.29.19 Criticality=true
1638          BasicConstraints:[
```

```
1639           CA:true
1640           PathLen:12
1641         ]
1642       },
1643       {
1644         ObjectId: 2.5.29.32 Criticality=false
1645         CertificatePolicies [
1646           [CertificatePolicyId: [2.5.29.32.0]
1647         [PolicyQualifierInfo: [
1648           qualifierID: 1.3.6.1.5.5.7.2.1
1649           qualifier: 0000: 16 1C 68 74 74 70 3A
     2F   2F 70 6F 6C 69 63 79 2E  ..http://policy.
1650         0010: 63 61 6D 65 72 66 69 72   6D 61 2E
     63 6F 6D        camerfirma.com
1651
1652         ]]  ]
1653         ]
1654       },
1655       {
1656         ObjectId: 2.5.29.15 Criticality=true
1657         KeyUsage [
1658           Key_CertSign
1659           Crl_Sign
1660         ]
1661       },
1662       {
1663         ObjectId: 2.5.29.14 Criticality=false
1664         SubjectKeyIdentifier [
1665         KeyIdentifier [
1666         0000: F9 24 AC 0F B2 B5 F8 79   C0 FA 60
     88 1B C4 D9 4D  .$.....y..`....M
1667         0010: 02 9E 17 19
                                                ....
1668         ]
1669         ]
1670       }
1671     ]},
1672   "certificate" : {
1673     "version"            : "v3",
1674     "serial number"      : "56B629CD34BC78F6",
1675     "signature algorithm": "SHA256withRSA",
```

```
1676     "issuer"              : "CN=SSL.com EV Root
     Certification Authority RSA R2, O=SSL Corporation
     , L=Houston, ST=Texas, C=US",
1677     "not before"          : "2017-06-01 02:14:37.
     000 SGT",
1678     "not  after"          : "2042-05-31 02:14:37.
     000 SGT",
1679     "subject"             : "CN=SSL.com EV Root
     Certification Authority RSA R2, O=SSL Corporation
     , L=Houston, ST=Texas, C=US",
1680     "subject public key" : "RSA",
1681     "extensions"          : [
1682       {
1683         ObjectId: 2.5.29.35 Criticality=false
1684         AuthorityKeyIdentifier [
1685         KeyIdentifier [
1686         0000: F9 60 BB D4 E3 D5 34 F6   B8 F5 06
     80 25 A7 73 DB  .`....4.....%.s.
1687         0010: 46 69 A8 9E
                                             Fi..
1688         ]
1689         ]
1690       },
1691       {
1692         ObjectId: 2.5.29.19 Criticality=true
1693         BasicConstraints:[
1694           CA:true
1695           PathLen: no limit
1696         ]
1697       },
1698       {
1699         ObjectId: 2.5.29.15 Criticality=true
1700         KeyUsage [
1701           DigitalSignature
1702           Key_CertSign
1703           Crl_Sign
1704         ]
1705       },
1706       {
1707         ObjectId: 2.5.29.14 Criticality=false
1708         SubjectKeyIdentifier [
```

```
1709         KeyIdentifier [
1710         0000: F9 60 BB D4 E3 D5 34 F6   B8 F5 06
     80 25 A7 73 DB  .`....4.....%.s.
1711         0010: 46 69 A8 9E
                                            Fi..
1712         ]
1713         ]
1714       }
1715     ]},
1716   "certificate" : {
1717     "version"            : "v3",
1718     "serial number"      : "4F1BD42F54BB2F4B",
1719     "signature algorithm": "SHA1withRSA",
1720     "issuer"             : "CN=SwissSign Silver
     CA - G2, O=SwissSign AG, C=CH",
1721     "not before"         : "2006-10-25 16:32:46.
     000 SGT",
1722     "not  after"         : "2036-10-25 16:32:46.
     000 SGT",
1723     "subject"            : "CN=SwissSign Silver
     CA - G2, O=SwissSign AG, C=CH",
1724     "subject public key" : "RSA",
1725     "extensions"         : [
1726       {
1727         ObjectId: 2.5.29.35 Criticality=false
1728         AuthorityKeyIdentifier [
1729         KeyIdentifier [
1730         0000: 17 A0 CD C1 E4 41 B6 3A   5B 3B CB
     45 9D BD 1C C2  .....A.:[;.E....
1731         0010: 98 FA 86 58
                                            ...X
1732         ]
1733         ]
1734       },
1735       {
1736         ObjectId: 2.5.29.19 Criticality=true
1737         BasicConstraints:[
1738           CA:true
1739           PathLen: no limit
1740         ]
1741       },
```

```
1742       {
1743         ObjectId: 2.5.29.32 Criticality=false
1744         CertificatePolicies [
1745           [CertificatePolicyId: [2.16.756.1.89.1.
     3.1.1]
1746         [PolicyQualifierInfo: [
1747           qualifierID: 1.3.6.1.5.5.7.2.1
1748           qualifier: 0000: 16 20 68 74 74 70 3A
     2F   2F 72 65 70 6F 73 69 74  . http://reposit
1749         0010: 6F 72 79 2E 73 77 69 73   73 73 69
     67 6E 2E 63 6F  ory.swisssign.co
1750         0020: 6D 2F
                                                 m/
1751
1752         ]]  ]
1753         ]
1754       },
1755       {
1756         ObjectId: 2.5.29.15 Criticality=true
1757         KeyUsage [
1758           Key_CertSign
1759           Crl_Sign
1760         ]
1761       },
1762       {
1763         ObjectId: 2.5.29.14 Criticality=false
1764         SubjectKeyIdentifier [
1765         KeyIdentifier [
1766         0000: 17 A0 CD C1 E4 41 B6 3A   5B 3B CB
     45 9D BD 1C C2  .....A.:[;.E....
1767         0010: 98 FA 86 58
                                             ...X
1768         ]
1769         ]
1770       }
1771     ]},
1772   "certificate" : {
1773     "version"            : "v3",
1774     "serial number"      : "75E6DFCBC1685BA8",
1775     "signature algorithm": "SHA256withECDSA",
1776     "issuer"             : "CN=SSL.com Root
```

```
1776 Certification Authority ECC, O=SSL Corporation, L
     =Houston, ST=Texas, C=US",
1777     "not before"         : "2016-02-13 02:14:03.
     000 SGT",
1778     "not  after"         : "2041-02-13 02:14:03.
     000 SGT",
1779     "subject"            : "CN=SSL.com Root
     Certification Authority ECC, O=SSL Corporation, L
     =Houston, ST=Texas, C=US",
1780     "subject public key" : "EC",
1781     "extensions"         : [
1782       {
1783         ObjectId: 2.5.29.35 Criticality=false
1784         AuthorityKeyIdentifier [
1785         KeyIdentifier [
1786         0000: 82 D1 85 73 30 E7 35 04   D3 8E 02
     92 FB E5 A4 D1  ...s0.5.........
1787         0010: C4 21 E8 CD
                                             .!..
1788         ]
1789         ]
1790       },
1791       {
1792         ObjectId: 2.5.29.19 Criticality=true
1793         BasicConstraints:[
1794           CA:true
1795           PathLen: no limit
1796         ]
1797       },
1798       {
1799         ObjectId: 2.5.29.15 Criticality=true
1800         KeyUsage [
1801           DigitalSignature
1802           Key_CertSign
1803           Crl_Sign
1804         ]
1805       },
1806       {
1807         ObjectId: 2.5.29.14 Criticality=false
1808         SubjectKeyIdentifier [
1809         KeyIdentifier [
```

```
1810         0000: 82 D1 85 73 30 E7 35 04   D3 8E 02
     92 FB E5 A4 D1  ...s0.5.........
1811         0010: C4 21 E8 CD
                                             .!..
1812         ]
1813         ]
1814       }
1815     ]},
1816   "certificate" : {
1817     "version"            : "v3",
1818     "serial number"      : "4A538C28",
1819     "signature algorithm": "SHA256withRSA",
1820     "issuer"             : "CN=Entrust Root
     Certification Authority - G2, OU="(c) 2009
     Entrust, Inc. - for authorized use only", OU=See
     www.entrust.net/legal-terms, O="Entrust, Inc.", C
     =US",
1821     "not before"         : "2009-07-08 01:25:54.
     000 SGT",
1822     "not  after"         : "2030-12-08 01:55:54.
     000 SGT",
1823     "subject"            : "CN=Entrust Root
     Certification Authority - G2, OU="(c) 2009
     Entrust, Inc. - for authorized use only", OU=See
     www.entrust.net/legal-terms, O="Entrust, Inc.", C
     =US",
1824     "subject public key" : "RSA",
1825     "extensions"         : [
1826       {
1827         ObjectId: 2.5.29.19 Criticality=true
1828         BasicConstraints:[
1829           CA:true
1830           PathLen: no limit
1831         ]
1832       },
1833       {
1834         ObjectId: 2.5.29.15 Criticality=true
1835         KeyUsage [
1836           Key_CertSign
1837           Crl_Sign
1838         ]
```

```
1839       },
1840       {
1841         ObjectId: 2.5.29.14 Criticality=false
1842         SubjectKeyIdentifier [
1843         KeyIdentifier [
1844         0000: 6A 72 26 7A D0 1E EF 7D   E7 3B 69
     51 D4 6C 8D 9F  jr&z.....;iQ.l..
1845         0010: 90 12 66 AB
                                                ..f.
1846         ]
1847         ]
1848       }
1849     ]},
1850   "certificate" : {
1851     "version"            : "v3",
1852     "serial number"      : "
     0CE7E0E517D846FE8FE560FC1BF03039",
1853     "signature algorithm": "SHA1withRSA",
1854     "issuer"             : "CN=DigiCert Assured
     ID Root CA, OU=www.digicert.com, O=DigiCert Inc,
     C=US",
1855     "not before"         : "2006-11-10 08:00:00.
     000 SGT",
1856     "not  after"         : "2031-11-10 08:00:00.
     000 SGT",
1857     "subject"            : "CN=DigiCert Assured
     ID Root CA, OU=www.digicert.com, O=DigiCert Inc,
     C=US",
1858     "subject public key" : "RSA",
1859     "extensions"         : [
1860       {
1861         ObjectId: 2.5.29.35 Criticality=false
1862         AuthorityKeyIdentifier [
1863         KeyIdentifier [
1864         0000: 45 EB A2 AF F4 92 CB 82   31 2D 51
     8B A7 A7 21 9D  E.......1-Q...!.
1865         0010: F3 6D C8 0F
                                                .m..
1866         ]
1867         ]
1868       },
```

```
1869       {
1870         ObjectId: 2.5.29.19 Criticality=true
1871         BasicConstraints:[
1872           CA:true
1873           PathLen: no limit
1874         ]
1875       },
1876       {
1877         ObjectId: 2.5.29.15 Criticality=true
1878         KeyUsage [
1879           DigitalSignature
1880           Key_CertSign
1881           Crl_Sign
1882         ]
1883       },
1884       {
1885         ObjectId: 2.5.29.14 Criticality=false
1886         SubjectKeyIdentifier [
1887         KeyIdentifier [
1888         0000: 45 EB A2 AF F4 92 CB 82   31 2D 51
     8B A7 A7 21 9D  E.......1-Q...!.
1889         0010: F3 6D C8 0F
                                                .m..
1890         ]
1891         ]
1892       }
1893     ]},
1894   "certificate" : {
1895     "version"            : "v3",
1896     "serial number"      : "00",
1897     "signature algorithm": "SHA1withRSA",
1898     "issuer"             : "OU=Go Daddy Class 2
     Certification Authority, O="The Go Daddy Group,
     Inc.", C=US",
1899     "not before"         : "2004-06-30 01:06:20.
     000 SGT",
1900     "not  after"         : "2034-06-30 01:06:20.
     000 SGT",
1901     "subject"            : "OU=Go Daddy Class 2
     Certification Authority, O="The Go Daddy Group,
     Inc.", C=US",
```

```
1902     "subject public key" : "RSA",
1903     "extensions"         : [
1904       {
1905         ObjectId: 2.5.29.35 Criticality=false
1906         AuthorityKeyIdentifier [
1907         KeyIdentifier [
1908         0000: D2 C4 B0 D2 91 D4 4C 11   71 B3 61
     CB 3D A1 FE DD  ......L.q.a.=...
1909         0010: A8 6A D4 E3
                                            .j..
1910         ]
1911         [OU=Go Daddy Class 2 Certification
     Authority, O="The Go Daddy Group, Inc.", C=US]
1912         SerialNumber: [    00]
1913         ]
1914       },
1915       {
1916         ObjectId: 2.5.29.19 Criticality=false
1917         BasicConstraints:[
1918           CA:true
1919           PathLen: no limit
1920         ]
1921       },
1922       {
1923         ObjectId: 2.5.29.14 Criticality=false
1924         SubjectKeyIdentifier [
1925         KeyIdentifier [
1926         0000: D2 C4 B0 D2 91 D4 4C 11   71 B3 61
     CB 3D A1 FE DD  ......L.q.a.=...
1927         0010: A8 6A D4 E3
                                            .j..
1928         ]
1929         ]
1930       }
1931     ]},
1932   "certificate" : {
1933     "version"            : "v3",
1934     "serial number"      : "01",
1935     "signature algorithm": "SHA1withRSA",
1936     "issuer"             : "CN=AddTrust External
     CA Root, OU=AddTrust External TTP Network, O=
```

```
1936 AddTrust AB, C=SE",
1937     "not before"         : "2000-05-30 18:48:38.
     000 SGT",
1938     "not  after"         : "2020-05-30 18:48:38.
     000 SGT",
1939     "subject"            : "CN=AddTrust External
     CA Root, OU=AddTrust External TTP Network, O=
     AddTrust AB, C=SE",
1940     "subject public key" : "RSA",
1941     "extensions"         : [
1942       {
1943         ObjectId: 2.5.29.35 Criticality=false
1944         AuthorityKeyIdentifier [
1945         KeyIdentifier [
1946         0000: AD BD 98 7A 34 B4 26 F7   FA C4 26
     54 EF 03 BD E0  ...z4.&...&T....
1947         0010: 24 CB 54 1A
                                             $.T.
1948         ]
1949         [CN=AddTrust External CA Root, OU=
     AddTrust External TTP Network, O=AddTrust AB, C=
     SE]
1950         SerialNumber: [    01]
1951         ]
1952       },
1953       {
1954         ObjectId: 2.5.29.19 Criticality=true
1955         BasicConstraints:[
1956           CA:true
1957           PathLen: no limit
1958         ]
1959       },
1960       {
1961         ObjectId: 2.5.29.15 Criticality=false
1962         KeyUsage [
1963           Key_CertSign
1964           Crl_Sign
1965         ]
1966       },
1967       {
1968         ObjectId: 2.5.29.14 Criticality=false
```

```
1969         SubjectKeyIdentifier [
1970         KeyIdentifier [
1971         0000: AD BD 98 7A 34 B4 26 F7   FA C4 26
     54 EF 03 BD E0  ...z4.&...&T....
1972         0010: 24 CB 54 1A
                                            $.T.
1973         ]
1974         ]
1975       }
1976     ]},
1977   "certificate" : {
1978     "version"            : "v3",
1979     "serial number"      : "
     0203E5936F31B01349886BA217",
1980     "signature algorithm": "SHA384withRSA",
1981     "issuer"             : "CN=GTS Root R1, O=
     Google Trust Services LLC, C=US",
1982     "not before"         : "2016-06-22 08:00:00.
     000 SGT",
1983     "not  after"         : "2036-06-22 08:00:00.
     000 SGT",
1984     "subject"            : "CN=GTS Root R1, O=
     Google Trust Services LLC, C=US",
1985     "subject public key" : "RSA",
1986     "extensions"         : [
1987       {
1988         ObjectId: 2.5.29.19 Criticality=true
1989         BasicConstraints:[
1990           CA:true
1991           PathLen: no limit
1992         ]
1993       },
1994       {
1995         ObjectId: 2.5.29.15 Criticality=true
1996         KeyUsage [
1997           DigitalSignature
1998           Key_CertSign
1999           Crl_Sign
2000         ]
2001       },
2002       {
```

```
2003         ObjectId: 2.5.29.14 Criticality=false
2004         SubjectKeyIdentifier [
2005         KeyIdentifier [
2006         0000: E4 AF 2B 26 71 1A 2B 48   27 85 2F
     52 66 2C EF F0  ..+&q.+H'./Rf,..
2007         0010: 89 13 71 3E
                                            ..q>
2008         ]
2009         ]
2010       }
2011     ]},
2012   "certificate" : {
2013     "version"            : "v3",
2014     "serial number"      : "01",
2015     "signature algorithm": "SHA256withRSA",
2016     "issuer"             : "CN=T-TeleSec
     GlobalRoot Class 3, OU=T-Systems Trust Center, O=
     T-Systems Enterprise Services GmbH, C=DE",
2017     "not before"         : "2008-10-01 18:29:56.
     000 SGT",
2018     "not  after"         : "2033-10-02 07:59:59.
     000 SGT",
2019     "subject"            : "CN=T-TeleSec
     GlobalRoot Class 3, OU=T-Systems Trust Center, O=
     T-Systems Enterprise Services GmbH, C=DE",
2020     "subject public key" : "RSA",
2021     "extensions"         : [
2022       {
2023         ObjectId: 2.5.29.19 Criticality=true
2024         BasicConstraints:[
2025           CA:true
2026           PathLen: no limit
2027         ]
2028       },
2029       {
2030         ObjectId: 2.5.29.15 Criticality=true
2031         KeyUsage [
2032           Key_CertSign
2033           Crl_Sign
2034         ]
2035       },
```

```
2036       {
2037         ObjectId: 2.5.29.14 Criticality=false
2038         SubjectKeyIdentifier [
2039         KeyIdentifier [
2040         0000: B5 03 F7 76 3B 61 82 6A   12 AA 18
     53 EB 03 21 94  ...v;a.j...S..!.
2041         0010: BF FE CE CA
                                                 ....
2042         ]
2043         ]
2044       }
2045     ]},
2046   "certificate" : {
2047     "version"            : "v3",
2048     "serial number"      : "
     00CAE91B89F155030DA3E6416DC4E3A6E1",
2049     "signature algorithm": "SHA256withRSA",
2050     "issuer"             : "CN=Certigna Root CA,
     OU=0002 48146308100036, O=Dhimyotis, C=FR",
2051     "not before"         : "2013-10-01 16:32:27.
     000 SGT",
2052     "not  after"         : "2033-10-01 16:32:27.
     000 SGT",
2053     "subject"            : "CN=Certigna Root CA,
     OU=0002 48146308100036, O=Dhimyotis, C=FR",
2054     "subject public key" : "RSA",
2055     "extensions"         : [
2056       {
2057         ObjectId: 2.5.29.35 Criticality=false
2058         AuthorityKeyIdentifier [
2059         KeyIdentifier [
2060         0000: 18 87 56 E0 6E 77 EE 24   35 3C 4E
     73 9A 1F D6 E1  ..V.nw.$5<Ns....
2061         0010: E2 79 7E 2B
                                                 .y.+
2062         ]
2063         ]
2064       },
2065       {
2066         ObjectId: 2.5.29.19 Criticality=true
2067         BasicConstraints:[
```

```
2068           CA:true
2069           PathLen: no limit
2070         ]
2071       },
2072       {
2073         ObjectId: 2.5.29.31 Criticality=false
2074         CRLDistributionPoints [
2075           [DistributionPoint:
2076              [URIName: http://crl.certigna.fr/
     certignarootca.crl]
2077         , DistributionPoint:
2078              [URIName: http://crl.dhimyotis.com/
     certignarootca.crl]
2079         ]]
2080       },
2081       {
2082         ObjectId: 2.5.29.32 Criticality=false
2083         CertificatePolicies [
2084           [CertificatePolicyId: [2.5.29.32.0]
2085         [PolicyQualifierInfo: [
2086           qualifierID: 1.3.6.1.5.5.7.2.1
2087           qualifier: 0000: 16 23 68 74 74 70 73
     3A   2F 2F 77 77 77 77 2E 63  .#https://wwww.c
2088         0010: 65 72 74 69 67 6E 61 2E   66 72 2F
     61 75 74 6F 72  ertigna.fr/autor
2089         0020: 69 74 65 73 2F
                                             ites/
2090
2091         ]]  ]
2092         ]
2093       },
2094       {
2095         ObjectId: 2.5.29.15 Criticality=true
2096         KeyUsage [
2097           Key_CertSign
2098           Crl_Sign
2099         ]
2100       },
2101       {
2102         ObjectId: 2.5.29.14 Criticality=false
2103         SubjectKeyIdentifier [
```

```
2104         KeyIdentifier [
2105         0000: 18 87 56 E0 6E 77 EE 24   35 3C 4E
     73 9A 1F D6 E1  ..V.nw.$5<Ns....
2106         0010: E2 79 7E 2B
                                            .y.+
2107         ]
2108         ]
2109       }
2110     ]},
2111   "certificate" : {
2112     "version"            : "v3",
2113     "serial number"      : "
     055556BCF25EA43535C3A40FD5AB4572",
2114     "signature algorithm": "SHA384withECDSA",
2115     "issuer"             : "CN=DigiCert Global
     Root G3, OU=www.digicert.com, O=DigiCert Inc, C=
     US",
2116     "not before"         : "2013-08-01 20:00:00.
     000 SGT",
2117     "not  after"         : "2038-01-15 20:00:00.
     000 SGT",
2118     "subject"            : "CN=DigiCert Global
     Root G3, OU=www.digicert.com, O=DigiCert Inc, C=
     US",
2119     "subject public key" : "EC",
2120     "extensions"         : [
2121       {
2122         ObjectId: 2.5.29.19 Criticality=true
2123         BasicConstraints:[
2124           CA:true
2125           PathLen: no limit
2126         ]
2127       },
2128       {
2129         ObjectId: 2.5.29.15 Criticality=true
2130         KeyUsage [
2131           DigitalSignature
2132           Key_CertSign
2133           Crl_Sign
2134         ]
2135       },
```

```
2136        {
2137          ObjectId: 2.5.29.14 Criticality=false
2138          SubjectKeyIdentifier [
2139          KeyIdentifier [
2140          0000: B3 DB 48 A4 F9 A1 C5 D8   AE 36 41
     CC 11 63 69 62  ..H......6A..cib
2141          0010: 29 BC 4B C6
                                              ).K.
2142          ]
2143          ]
2144        }
2145      ]},
2146    "certificate" : {
2147      "version"            : "v3",
2148      "serial number"      : "
     08F9B478A8FA7EDA6A333789DE7CCF8A",
2149      "signature algorithm": "SHA384withRSA",
2150      "issuer"             : "CN=DigiCert TLS
     RSA4096 Root G5, O="DigiCert, Inc.", C=US",
2151      "not before"         : "2021-01-15 08:00:00.
     000 SGT",
2152      "not  after"         : "2046-01-15 07:59:59.
     000 SGT",
2153      "subject"            : "CN=DigiCert TLS
     RSA4096 Root G5, O="DigiCert, Inc.", C=US",
2154      "subject public key" : "RSA",
2155      "extensions"         : [
2156        {
2157          ObjectId: 2.5.29.19 Criticality=true
2158          BasicConstraints:[
2159            CA:true
2160            PathLen: no limit
2161          ]
2162        },
2163        {
2164          ObjectId: 2.5.29.15 Criticality=true
2165          KeyUsage [
2166            DigitalSignature
2167            Key_CertSign
2168            Crl_Sign
2169          ]
```

```
2170       },
2171       {
2172         ObjectId: 2.5.29.14 Criticality=false
2173         SubjectKeyIdentifier [
2174         KeyIdentifier [
2175         0000: 51 33 1C ED 36 40 AF 17   D3 25 CD
     69 68 F2 AF 4E  Q3..6@...%.ih..N
2176         0010: 23 3E B3 41
                                                #>.A
2177         ]
2178         ]
2179       }
2180     ]},
2181   "certificate" : {
2182     "version"            : "v3",
2183     "serial number"      : "023456",
2184     "signature algorithm": "SHA1withRSA",
2185     "issuer"             : "CN=GeoTrust Global CA
     , O=GeoTrust Inc., C=US",
2186     "not before"         : "2002-05-21 12:00:00.
     000 SGT",
2187     "not  after"         : "2022-05-21 12:00:00.
     000 SGT",
2188     "subject"            : "CN=GeoTrust Global CA
     , O=GeoTrust Inc., C=US",
2189     "subject public key" : "RSA",
2190     "extensions"         : [
2191       {
2192         ObjectId: 2.5.29.35 Criticality=false
2193         AuthorityKeyIdentifier [
2194         KeyIdentifier [
2195         0000: C0 7A 98 68 8D 89 FB AB   05 64 0C
     11 7D AA 7D 65  .z.h.....d.....e
2196         0010: B8 CA CC 4E
                                                ...N
2197         ]
2198         ]
2199       },
2200       {
2201         ObjectId: 2.5.29.19 Criticality=true
2202         BasicConstraints:[
```

```
2203           CA:true
2204           PathLen: no limit
2205         ]
2206       },
2207       {
2208         ObjectId: 2.5.29.14 Criticality=false
2209         SubjectKeyIdentifier [
2210         KeyIdentifier [
2211         0000: C0 7A 98 68 8D 89 FB AB   05 64 0C
     11 7D AA 7D 65  .z.h.....d.....e
2212         0010: B8 CA CC 4E
                                                ...N
2213         ]
2214         ]
2215       }
2216     ]},
2217   "certificate" : {
2218     "version"            : "v3",
2219     "serial number"      : "4EB200670C035D4F",
2220     "signature algorithm": "SHA1withRSA",
2221     "issuer"             : "CN=SwissSign Platinum
      CA - G2, O=SwissSign AG, C=CH",
2222     "not before"         : "2006-10-25 16:36:00.
     000 SGT",
2223     "not  after"         : "2036-10-25 16:36:00.
     000 SGT",
2224     "subject"            : "CN=SwissSign Platinum
      CA - G2, O=SwissSign AG, C=CH",
2225     "subject public key" : "RSA",
2226     "extensions"         : [
2227       {
2228         ObjectId: 2.5.29.35 Criticality=false
2229         AuthorityKeyIdentifier [
2230         KeyIdentifier [
2231         0000: 50 AF CC 07 87 15 47 6F   38 C5 B4
     65 D1 DE 95 AA  P.....Go8..e....
2232         0010: E9 DF 9C CC
                                                ....
2233         ]
2234         ]
2235       },
```

```
2236        {
2237          ObjectId: 2.5.29.19 Criticality=true
2238          BasicConstraints:[
2239            CA:true
2240            PathLen: no limit
2241          ]
2242        },
2243        {
2244          ObjectId: 2.5.29.32 Criticality=false
2245          CertificatePolicies [
2246            [CertificatePolicyId: [2.16.756.1.89.1.
     1.1.1]
2247          [PolicyQualifierInfo: [
2248            qualifierID: 1.3.6.1.5.5.7.2.1
2249            qualifier: 0000: 16 20 68 74 74 70 3A
     2F   2F 72 65 70 6F 73 69 74  . http://reposit
2250          0010: 6F 72 79 2E 73 77 69 73   73 73 69
     67 6E 2E 63 6F  ory.swisssign.co
2251          0020: 6D 2F
                                                  m/
2252
2253          ]]  ]
2254          ]
2255        },
2256        {
2257          ObjectId: 2.5.29.15 Criticality=true
2258          KeyUsage [
2259            Key_CertSign
2260            Crl_Sign
2261          ]
2262        },
2263        {
2264          ObjectId: 2.5.29.14 Criticality=false
2265          SubjectKeyIdentifier [
2266          KeyIdentifier [
2267          0000: 50 AF CC 07 87 15 47 6F   38 C5 B4
     65 D1 DE 95 AA  P.....Go8..e....
2268          0010: E9 DF 9C CC
                                              ....
2269          ]
2270          ]
```

```
2271        }
2272      ]},
2273    "certificate" : {
2274      "version"            : "v3",
2275      "serial number"      : "
      605949E0262EBB55F90A778A71F94AD86C",
2276      "signature algorithm": "SHA384withECDSA",
2277      "issuer"             : "CN=GlobalSign, O=
      GlobalSign, OU=GlobalSign ECC Root CA - R5",
2278      "not before"         : "2012-11-13 08:00:00.
      000 SGT",
2279      "not  after"         : "2038-01-19 11:14:07.
      000 SGT",
2280      "subject"            : "CN=GlobalSign, O=
      GlobalSign, OU=GlobalSign ECC Root CA - R5",
2281      "subject public key" : "EC",
2282      "extensions"         : [
2283        {
2284          ObjectId: 2.5.29.19 Criticality=true
2285          BasicConstraints:[
2286            CA:true
2287            PathLen: no limit
2288          ]
2289        },
2290        {
2291          ObjectId: 2.5.29.15 Criticality=true
2292          KeyUsage [
2293            Key_CertSign
2294            Crl_Sign
2295          ]
2296        },
2297        {
2298          ObjectId: 2.5.29.14 Criticality=false
2299          SubjectKeyIdentifier [
2300          KeyIdentifier [
2301          0000: 3D E6 29 48 9B EA 07 CA   21 44 4A
      26 DE 6E DE D2  =.)H....!DJ&.n..
2302          0010: 83 D0 9F 59
                                                ...Y
2303          ]
2304          ]
```

```
2305       }
2306     ]},
2307   "certificate" : {
2308     "version"            : "v3",
2309     "serial number"      : "00",
2310     "signature algorithm": "SHA256withRSA",
2311     "issuer"             : "CN=Starfield Root
     Certificate Authority - G2, O="Starfield
     Technologies, Inc.", L=Scottsdale, ST=Arizona, C=
     US",
2312     "not before"         : "2009-09-01 08:00:00.
     000 SGT",
2313     "not  after"         : "2038-01-01 07:59:59.
     000 SGT",
2314     "subject"            : "CN=Starfield Root
     Certificate Authority - G2, O="Starfield
     Technologies, Inc.", L=Scottsdale, ST=Arizona, C=
     US",
2315     "subject public key" : "RSA",
2316     "extensions"         : [
2317       {
2318         ObjectId: 2.5.29.19 Criticality=true
2319         BasicConstraints:[
2320           CA:true
2321           PathLen: no limit
2322         ]
2323       },
2324       {
2325         ObjectId: 2.5.29.15 Criticality=true
2326         KeyUsage [
2327           Key_CertSign
2328           Crl_Sign
2329         ]
2330       },
2331       {
2332         ObjectId: 2.5.29.14 Criticality=false
2333         SubjectKeyIdentifier [
2334         KeyIdentifier [
2335         0000: 7C 0C 32 1F A7 D9 30 7F   C4 7D 68
     A3 62 A8 A1 CE  ..2...0...h.b...
2336         0010: AB 07 5B 27
```

```
                                                ..['
        ]
        ]
      }
    ]},
  "certificate" : {
    "version"            : "v3",
    "serial number"      : "
    0A01428000000014523CF467C00000002",
    "signature algorithm": "SHA256withRSA",
    "issuer"             : "CN=IdenTrust Public
    Sector Root CA 1, O=IdenTrust, C=US",
    "not before"         : "2014-01-17 01:53:32.
    000 SGT",
    "not  after"         : "2034-01-17 01:53:32.
    000 SGT",
    "subject"            : "CN=IdenTrust Public
    Sector Root CA 1, O=IdenTrust, C=US",
    "subject public key" : "RSA",
    "extensions"         : [
      {
        ObjectId: 2.5.29.19 Criticality=true
        BasicConstraints:[
          CA:true
          PathLen: no limit
        ]
      },
      {
        ObjectId: 2.5.29.15 Criticality=true
        KeyUsage [
          Key_CertSign
          Crl_Sign
        ]
      },
      {
        ObjectId: 2.5.29.14 Criticality=false
        SubjectKeyIdentifier [
        KeyIdentifier [
        0000: E3 71 E0 9E D8 A7 42 D9   DB 71 91
    6B 94 93 EB C3  .q....B..q.k....
        0010: A3 D1 14 A3
```

```
2370                                                    ....
2371          ]
2372          ]
2373        }
2374      ]},
2375    "certificate" : {
2376      "version"            : "v3",
2377      "serial number"      : "3863DEF8",
2378      "signature algorithm": "SHA1withRSA",
2379      "issuer"             : "CN=Entrust.net
     Certification Authority (2048), OU=(c) 1999
     Entrust.net Limited, OU=www.entrust.net/CPS_2048
     incorp. by ref. (limits liab.), O=Entrust.net",
2380      "not before"         : "1999-12-25 01:50:51.
     000 SGT",
2381      "not  after"         : "2029-07-24 22:15:12.
     000 SGT",
2382      "subject"            : "CN=Entrust.net
     Certification Authority (2048), OU=(c) 1999
     Entrust.net Limited, OU=www.entrust.net/CPS_2048
     incorp. by ref. (limits liab.), O=Entrust.net",
2383      "subject public key" : "RSA",
2384      "extensions"         : [
2385        {
2386          ObjectId: 2.5.29.19 Criticality=true
2387          BasicConstraints:[
2388            CA:true
2389            PathLen: no limit
2390          ]
2391        },
2392        {
2393          ObjectId: 2.5.29.15 Criticality=true
2394          KeyUsage [
2395            Key_CertSign
2396            Crl_Sign
2397          ]
2398        },
2399        {
2400          ObjectId: 2.5.29.14 Criticality=false
2401          SubjectKeyIdentifier [
2402          KeyIdentifier [
```

```
2403          0000: 55 E4 81 D1 11 80 BE D8   89 B9 08
     A3 31 F9 A1 24  U...........1..$
2404          0010: 09 16 B9 70
                                              ...p
2405          ]
2406          ]
2407        }
2408      ]},
2409    "certificate" : {
2410      "version"            : "v3",
2411      "serial number"      : "
     00864DBF0FE35ED77D8ED8",
2412      "signature algorithm": "SHA384withRSA",
2413      "issuer"             : "CN=emSign Root CA -
     G2, O=eMudhra Technologies Limited, OU=emSign PKI
     , C=IN",
2414      "not before"         : "2018-02-19 02:30:00.
     000 SGT",
2415      "not  after"         : "2043-02-19 02:30:00.
     000 SGT",
2416      "subject"            : "CN=emSign Root CA -
     G2, O=eMudhra Technologies Limited, OU=emSign PKI
     , C=IN",
2417      "subject public key" : "RSA",
2418      "extensions"         : [
2419        {
2420          ObjectId: 2.5.29.19 Criticality=true
2421          BasicConstraints:[
2422            CA:true
2423            PathLen: no limit
2424          ]
2425        },
2426        {
2427          ObjectId: 2.5.29.15 Criticality=true
2428          KeyUsage [
2429            Key_CertSign
2430            Crl_Sign
2431          ]
2432        },
2433        {
2434          ObjectId: 2.5.29.14 Criticality=false
```

```
2435         SubjectKeyIdentifier [
2436         KeyIdentifier [
2437         0000: ED EC 4D 45 61 18 28 E7   B3 23 28
     11 1C 4D A5 27  ..MEa.(..#(..M.'
2438         0010: 0D 5E EC F4
                                                .^..
2439         ]
2440         ]
2441       }
2442     ]},
2443   "certificate" : {
2444     "version"            : "v3",
2445     "serial number"      : "
     0095BE16A0F72E46F17B398272FA8BCD96",
2446     "signature algorithm": "SHA1withRSA",
2447     "issuer"             : "CN=TeliaSonera Root
     CA v1, O=TeliaSonera",
2448     "not before"         : "2007-10-18 20:00:50.
     000 SGT",
2449     "not  after"         : "2032-10-18 20:00:50.
     000 SGT",
2450     "subject"            : "CN=TeliaSonera Root
     CA v1, O=TeliaSonera",
2451     "subject public key" : "RSA",
2452     "extensions"         : [
2453       {
2454         ObjectId: 2.5.29.19 Criticality=true
2455         BasicConstraints:[
2456           CA:true
2457           PathLen: no limit
2458         ]
2459       },
2460       {
2461         ObjectId: 2.5.29.15 Criticality=false
2462         KeyUsage [
2463           Key_CertSign
2464           Crl_Sign
2465         ]
2466       },
2467       {
2468         ObjectId: 2.5.29.14 Criticality=false
```

```
2469          SubjectKeyIdentifier [
2470          KeyIdentifier [
2471          0000: F0 8F 59 38 00 B3 F5 8F   9A 96 0C
     D5 EB FA 7B AA  ..Y8.............
2472          0010: 17 E8 13 12
                                              ....
2473          ]
2474          ]
2475        }
2476      ]},
2477    "certificate" : {
2478      "version"             : "v3",
2479      "serial number"       : "
     344ED55720D5EDEC49F42FCE37DB2B6D",
2480      "signature algorithm": "SHA1withRSA",
2481      "issuer"              : "CN=thawte Primary
     Root CA, OU="(c) 2006 thawte, Inc. - For
     authorized use only", OU=Certification Services
     Division, O="thawte, Inc.", C=US",
2482      "not before"          : "2006-11-17 08:00:00.
     000 SGT",
2483      "not  after"          : "2036-07-17 07:59:59.
     000 SGT",
2484      "subject"             : "CN=thawte Primary
     Root CA, OU="(c) 2006 thawte, Inc. - For
     authorized use only", OU=Certification Services
     Division, O="thawte, Inc.", C=US",
2485      "subject public key" : "RSA",
2486      "extensions"          : [
2487        {
2488          ObjectId: 2.5.29.19 Criticality=true
2489          BasicConstraints:[
2490            CA:true
2491            PathLen: no limit
2492          ]
2493        },
2494        {
2495          ObjectId: 2.5.29.15 Criticality=true
2496          KeyUsage [
2497            Key_CertSign
2498            Crl_Sign
```

```
2499          ]
2500        },
2501        {
2502          ObjectId: 2.5.29.14 Criticality=false
2503          SubjectKeyIdentifier [
2504          KeyIdentifier [
2505          0000: 7B 5B 45 CF AF CE CB 7A   FD 31 92
     1A 6A B6 F3 46  .[E....z.1..j..F
2506          0010: EB 57 48 50
                                              .WHP
2507          ]
2508          ]
2509        }
2510      ]},
2511    "certificate" : {
2512      "version"            : "v3",
2513      "serial number"      : "00",
2514      "signature algorithm": "SHA256withRSA",
2515      "issuer"             : "CN=Go Daddy Root
     Certificate Authority - G2, O="GoDaddy.com, Inc
     .", L=Scottsdale, ST=Arizona, C=US",
2516      "not before"         : "2009-09-01 08:00:00.
     000 SGT",
2517      "not  after"         : "2038-01-01 07:59:59.
     000 SGT",
2518      "subject"            : "CN=Go Daddy Root
     Certificate Authority - G2, O="GoDaddy.com, Inc
     .", L=Scottsdale, ST=Arizona, C=US",
2519      "subject public key" : "RSA",
2520      "extensions"         : [
2521        {
2522          ObjectId: 2.5.29.19 Criticality=true
2523          BasicConstraints:[
2524            CA:true
2525            PathLen: no limit
2526          ]
2527        },
2528        {
2529          ObjectId: 2.5.29.15 Criticality=true
2530          KeyUsage [
2531            Key_CertSign
```

```
2532           Crl_Sign
2533         ]
2534       },
2535       {
2536         ObjectId: 2.5.29.14 Criticality=false
2537         SubjectKeyIdentifier [
2538         KeyIdentifier [
2539         0000: 3A 9A 85 07 10 67 28 B6   EF F6 BD
     05 41 6E 20 C1  :....g(.....An .
2540         0010: 94 DA 0F DE
                                                ....
2541         ]
2542         ]
2543       }
2544     ]},
2545   "certificate" : {
2546     "version"            : "v3",
2547     "serial number"      : "
     2F80FE238C0E220F486712289187ACB3",
2548     "signature algorithm": "SHA384withECDSA",
2549     "issuer"             : "CN=VeriSign Class 3
     Public Primary Certification Authority - G4, OU
     ="(c) 2007 VeriSign, Inc. - For authorized use
     only", OU=VeriSign Trust Network, O="VeriSign,
     Inc.", C=US",
2550     "not before"         : "2007-11-05 08:00:00.
     000 SGT",
2551     "not  after"         : "2038-01-19 07:59:59.
     000 SGT",
2552     "subject"            : "CN=VeriSign Class 3
     Public Primary Certification Authority - G4, OU
     ="(c) 2007 VeriSign, Inc. - For authorized use
     only", OU=VeriSign Trust Network, O="VeriSign,
     Inc.", C=US",
2553     "subject public key" : "EC",
2554     "extensions"         : [
2555       {
2556         ObjectId: 1.3.6.1.5.5.7.1.12 Criticality=
     false
2557       },
2558       {
```

```
2559          ObjectId: 2.5.29.19 Criticality=true
2560          BasicConstraints:[
2561            CA:true
2562            PathLen: no limit
2563          ]
2564        },
2565        {
2566          ObjectId: 2.5.29.15 Criticality=true
2567          KeyUsage [
2568            Key_CertSign
2569            Crl_Sign
2570          ]
2571        },
2572        {
2573          ObjectId: 2.5.29.14 Criticality=false
2574          SubjectKeyIdentifier [
2575          KeyIdentifier [
2576          0000: B3 16 91 FD EE A6 6E E4   B5 2E 49
     8F 87 78 81 80  ......n...I..x..
2577          0010: EC E5 B1 B5
                                                ....
2578          ]
2579          ]
2580        }
2581      ]},
2582    "certificate" : {
2583      "version"            : "v3",
2584      "serial number"      : "
     0203E5B882EB20F825276D3D66",
2585      "signature algorithm": "SHA384withECDSA",
2586      "issuer"             : "CN=GTS Root R3, O=
     Google Trust Services LLC, C=US",
2587      "not before"         : "2016-06-22 08:00:00.
     000 SGT",
2588      "not  after"         : "2036-06-22 08:00:00.
     000 SGT",
2589      "subject"            : "CN=GTS Root R3, O=
     Google Trust Services LLC, C=US",
2590      "subject public key" : "EC",
2591      "extensions"         : [
2592        {
```

```
2593          ObjectId: 2.5.29.19 Criticality=true
2594          BasicConstraints:[
2595            CA:true
2596            PathLen: no limit
2597          ]
2598        },
2599        {
2600          ObjectId: 2.5.29.15 Criticality=true
2601          KeyUsage [
2602            DigitalSignature
2603            Key_CertSign
2604            Crl_Sign
2605          ]
2606        },
2607        {
2608          ObjectId: 2.5.29.14 Criticality=false
2609          SubjectKeyIdentifier [
2610          KeyIdentifier [
2611          0000: C1 F1 26 BA A0 2D AE 85   81 CF D3
     F1 2A 12 BD B8  ..&..-......*...
2612          0010: 0A 67 FD BC
                                                .g..
2613          ]
2614          ]
2615        }
2616      ]},
2617    "certificate" : {
2618      "version"            : "v3",
2619      "serial number"      : "456B5054",
2620      "signature algorithm": "SHA1withRSA",
2621      "issuer"             : "CN=Entrust Root
     Certification Authority, OU="(c) 2006 Entrust,
     Inc.", OU=www.entrust.net/CPS is incorporated by
     reference, O="Entrust, Inc.", C=US",
2622      "not before"         : "2006-11-28 04:23:42.
     000 SGT",
2623      "not  after"         : "2026-11-28 04:53:42.
     000 SGT",
2624      "subject"            : "CN=Entrust Root
     Certification Authority, OU="(c) 2006 Entrust,
     Inc.", OU=www.entrust.net/CPS is incorporated by
```

```
reference, O="Entrust, Inc.", C=US",
    "subject public key" : "RSA",
    "extensions"         : [
      {
        ObjectId: 1.2.840.113533.7.65.0
    Criticality=false
      },
      {
        ObjectId: 2.5.29.35 Criticality=false
        AuthorityKeyIdentifier [
        KeyIdentifier [
        0000: 68 90 E4 67 A4 A6 53 80   C7 86 66
    A4 F1 F7 4B 43  h..g..S...f...KC
        0010: FB 84 BD 6D
                                            ...m
        ]
        ]
      },
      {
        ObjectId: 2.5.29.19 Criticality=true
        BasicConstraints:[
          CA:true
          PathLen: no limit
        ]
      },
      {
        ObjectId: 2.5.29.15 Criticality=true
        KeyUsage [
          Key_CertSign
          Crl_Sign
        ]
      },
      {
        ObjectId: 2.5.29.16 Criticality=false
        PrivateKeyUsage: [
        From: Tue Nov 28 04:23:42 SGT 2006, To:
    Sat Nov 28 04:53:42 SGT 2026]
      },
      {
        ObjectId: 2.5.29.14 Criticality=false
        SubjectKeyIdentifier [
```

```
2661         KeyIdentifier [
2662         0000: 68 90 E4 67 A4 A6 53 80   C7 86 66
     A4 F1 F7 4B 43  h..g..S...f...KC
2663         0010: FB 84 BD 6D
                                                ...m
2664         ]
2665         ]
2666       }
2667     ]},
2668   "certificate" : {
2669     "version"            : "v3",
2670     "serial number"      : "
     0B931C3AD63967EA6723BFC3AF9AF44B",
2671     "signature algorithm": "SHA256withRSA",
2672     "issuer"             : "CN=DigiCert Assured
     ID Root G2, OU=www.digicert.com, O=DigiCert Inc,
     C=US",
2673     "not before"         : "2013-08-01 20:00:00.
     000 SGT",
2674     "not  after"         : "2038-01-15 20:00:00.
     000 SGT",
2675     "subject"            : "CN=DigiCert Assured
     ID Root G2, OU=www.digicert.com, O=DigiCert Inc,
     C=US",
2676     "subject public key" : "RSA",
2677     "extensions"         : [
2678       {
2679         ObjectId: 2.5.29.19 Criticality=true
2680         BasicConstraints:[
2681           CA:true
2682           PathLen: no limit
2683         ]
2684       },
2685       {
2686         ObjectId: 2.5.29.15 Criticality=true
2687         KeyUsage [
2688           DigitalSignature
2689           Key_CertSign
2690           Crl_Sign
2691         ]
2692       },
```

```
2693       {
2694         ObjectId: 2.5.29.14 Criticality=false
2695         SubjectKeyIdentifier [
2696         KeyIdentifier [
2697         0000: CE C3 4A B9 99 55 F2 B8   DB 60 BF
     A9 7E BD 56 B5  ..J..U...`....V.
2698         0010: 97 36 A7 D6
                                                .6..
2699         ]
2700         ]
2701       }
2702     ]},
2703   "certificate" : {
2704     "version"            : "v3",
2705     "serial number"      : "7B2C9BD316803299",
2706     "signature algorithm": "SHA256withRSA",
2707     "issuer"             : "CN=SSL.com Root
     Certification Authority RSA, O=SSL Corporation, L
     =Houston, ST=Texas, C=US",
2708     "not before"         : "2016-02-13 01:39:39.
     000 SGT",
2709     "not  after"         : "2041-02-13 01:39:39.
     000 SGT",
2710     "subject"            : "CN=SSL.com Root
     Certification Authority RSA, O=SSL Corporation, L
     =Houston, ST=Texas, C=US",
2711     "subject public key" : "RSA",
2712     "extensions"         : [
2713       {
2714         ObjectId: 2.5.29.35 Criticality=false
2715         AuthorityKeyIdentifier [
2716         KeyIdentifier [
2717         0000: DD 04 09 07 A2 F5 7A 7D   52 53 12
     92 95 EE 38 80  ......z.RS....8.
2718         0010: 25 0D A6 59
                                                %..Y
2719         ]
2720         ]
2721       },
2722       {
2723         ObjectId: 2.5.29.19 Criticality=true
```

```
2724          BasicConstraints:[
2725            CA:true
2726            PathLen: no limit
2727          ]
2728        },
2729        {
2730          ObjectId: 2.5.29.15 Criticality=true
2731          KeyUsage [
2732            DigitalSignature
2733            Key_CertSign
2734            Crl_Sign
2735          ]
2736        },
2737        {
2738          ObjectId: 2.5.29.14 Criticality=false
2739          SubjectKeyIdentifier [
2740          KeyIdentifier [
2741          0000: DD 04 09 07 A2 F5 7A 7D   52 53 12
     92 95 EE 38 80  ......z.RS....8.
2742          0010: 25 0D A6 59
                                            %..Y
2743          ]
2744          ]
2745        }
2746      ]},
2747    "certificate" : {
2748      "version"            : "v3",
2749      "serial number"      : "
     45E6BB038333C3856548E6FF4551",
2750      "signature algorithm": "SHA384withRSA",
2751      "issuer"             : "CN=GlobalSign, O=
     GlobalSign, OU=GlobalSign Root CA - R6",
2752      "not before"         : "2014-12-10 08:00:00.
     000 SGT",
2753      "not  after"         : "2034-12-10 08:00:00.
     000 SGT",
2754      "subject"            : "CN=GlobalSign, O=
     GlobalSign, OU=GlobalSign Root CA - R6",
2755      "subject public key" : "RSA",
2756      "extensions"         : [
2757        {
```

```
2758          ObjectId: 2.5.29.35 Criticality=false
2759          AuthorityKeyIdentifier [
2760          KeyIdentifier [
2761          0000: AE 6C 05 A3 93 13 E2 A2   E7 E2 D7
     1C D6 C7 F0 7F  .l.............
2762          0010: C8 67 53 A0
                                              .gS.
2763          ]
2764          ]
2765        },
2766        {
2767          ObjectId: 2.5.29.19 Criticality=true
2768          BasicConstraints:[
2769            CA:true
2770            PathLen: no limit
2771          ]
2772        },
2773        {
2774          ObjectId: 2.5.29.15 Criticality=true
2775          KeyUsage [
2776            Key_CertSign
2777            Crl_Sign
2778          ]
2779        },
2780        {
2781          ObjectId: 2.5.29.14 Criticality=false
2782          SubjectKeyIdentifier [
2783          KeyIdentifier [
2784          0000: AE 6C 05 A3 93 13 E2 A2   E7 E2 D7
     1C D6 C7 F0 7F  .l.............
2785          0010: C8 67 53 A0
                                              .gS.
2786          ]
2787          ]
2788        }
2789      ]},
2790    "certificate" : {
2791      "version"             : "v3",
2792      "serial number"       : "
     066C9FD7C1BB104C2943E5717B7B2CC81AC10E",
2793      "signature algorithm": "SHA384withECDSA",
```

```
2794     "issuer"              : "CN=Amazon Root CA 4,
     O=Amazon, C=US",
2795     "not before"          : "2015-05-26 08:00:00.
     000 SGT",
2796     "not  after"          : "2040-05-26 08:00:00.
     000 SGT",
2797     "subject"             : "CN=Amazon Root CA 4,
     O=Amazon, C=US",
2798     "subject public key" : "EC",
2799     "extensions"          : [
2800       {
2801         ObjectId: 2.5.29.19 Criticality=true
2802         BasicConstraints:[
2803           CA:true
2804           PathLen: no limit
2805         ]
2806       },
2807       {
2808         ObjectId: 2.5.29.15 Criticality=true
2809         KeyUsage [
2810           DigitalSignature
2811           Key_CertSign
2812           Crl_Sign
2813         ]
2814       },
2815       {
2816         ObjectId: 2.5.29.14 Criticality=false
2817         SubjectKeyIdentifier [
2818         KeyIdentifier [
2819         0000: D3 EC C7 3A 65 6E CC E1   DA 76 9A
     56 FB 9C F3 86  ...:en...v.V....
2820         0010: 6D 57 E5 81
                                                mW..
2821         ]
2822         ]
2823       }
2824     ]},
2825   "certificate" : {
2826     "version"             : "v3",
2827     "serial number"       : "010020",
2828     "signature algorithm": "SHA1withRSA",
```

```
2829     "issuer"              : "CN=Certum CA, O=
     Unizeto Sp. z o.o., C=PL",
2830     "not before"          : "2002-06-11 18:46:39.
     000 SGT",
2831     "not  after"          : "2027-06-11 18:46:39.
     000 SGT",
2832     "subject"             : "CN=Certum CA, O=
     Unizeto Sp. z o.o., C=PL",
2833     "subject public key" : "RSA",
2834     "extensions"          : [
2835       {
2836         ObjectId: 2.5.29.19 Criticality=true
2837         BasicConstraints:[
2838           CA:true
2839           PathLen: no limit
2840         ]
2841       }
2842     ]},
2843   "certificate" : {
2844     "version"             : "v3",
2845     "serial number"       : "01",
2846     "signature algorithm": "SHA1withRSA",
2847     "issuer"              : "CN=AddTrust Qualified
      CA Root, OU=AddTrust TTP Network, O=AddTrust AB
     , C=SE",
2848     "not before"          : "2000-05-30 18:44:50.
     000 SGT",
2849     "not  after"          : "2020-05-30 18:44:50.
     000 SGT",
2850     "subject"             : "CN=AddTrust Qualified
      CA Root, OU=AddTrust TTP Network, O=AddTrust AB
     , C=SE",
2851     "subject public key" : "RSA",
2852     "extensions"          : [
2853       {
2854         ObjectId: 2.5.29.35 Criticality=false
2855         AuthorityKeyIdentifier [
2856         KeyIdentifier [
2857         0000: 39 95 8B 62 8B 5C C9 D4   80 BA 58
     0F 97 3F 15 08  9..b.\....X..?..
2858         0010: 43 CC 98 A7
```

```
2858                                                C...
2859          ]
2860          [CN=AddTrust Qualified CA Root, OU=
     AddTrust TTP Network, O=AddTrust AB, C=SE]
2861          SerialNumber: [    01]
2862          ]
2863        },
2864        {
2865          ObjectId: 2.5.29.19 Criticality=true
2866          BasicConstraints:[
2867            CA:true
2868            PathLen: no limit
2869          ]
2870        },
2871        {
2872          ObjectId: 2.5.29.15 Criticality=false
2873          KeyUsage [
2874            Key_CertSign
2875            Crl_Sign
2876          ]
2877        },
2878        {
2879          ObjectId: 2.5.29.14 Criticality=false
2880          SubjectKeyIdentifier [
2881          KeyIdentifier [
2882          0000: 39 95 8B 62 8B 5C C9 D4   80 BA 58
     0F 97 3F 15 08  9..b.\....X..?..
2883          0010: 43 CC 98 A7
                                                    C...
2884          ]
2885          ]
2886        }
2887      ]},
2888    "certificate" : {
2889      "version"            : "v3",
2890      "serial number"      : "02",
2891      "signature algorithm": "SHA256withRSA",
2892      "issuer"             : "CN=Buypass Class 2
     Root CA, O=Buypass AS-983163327, C=NO",
2893      "not before"         : "2010-10-26 16:38:03.
     000 SGT",
```

```
2894     "not  after"          : "2040-10-26 16:38:03.
     000 SGT",
2895     "subject"             : "CN=Buypass Class 2
     Root CA, O=Buypass AS-983163327, C=NO",
2896     "subject public key" : "RSA",
2897     "extensions"          : [
2898       {
2899         ObjectId: 2.5.29.19 Criticality=true
2900         BasicConstraints:[
2901           CA:true
2902           PathLen: no limit
2903         ]
2904       },
2905       {
2906         ObjectId: 2.5.29.15 Criticality=true
2907         KeyUsage [
2908           Key_CertSign
2909           Crl_Sign
2910         ]
2911       },
2912       {
2913         ObjectId: 2.5.29.14 Criticality=false
2914         SubjectKeyIdentifier [
2915         KeyIdentifier [
2916         0000: C9 80 77 E0 62 92 82 F5   46 9C F3
     BA F7 4C C3 DE  ..w.b...F....L..
2917         0010: B8 A3 AD 39
                                                ...9
2918         ]
2919         ]
2920       }
2921     ]},
2922   "certificate" : {
2923     "version"             : "v3",
2924     "serial number"       : "0983F4",
2925     "signature algorithm": "SHA256withRSA",
2926     "issuer"              : "CN=D-TRUST Root Class
      3 CA 2 EV 2009, O=D-Trust GmbH, C=DE",
2927     "not before"          : "2009-11-05 16:50:46.
     000 SGT",
2928     "not  after"          : "2029-11-05 16:50:46.
```

```
2928 000 SGT",
2929     "subject"            : "CN=D-TRUST Root Class
      3 CA 2 EV 2009, O=D-Trust GmbH, C=DE",
2930     "subject public key" : "RSA",
2931     "extensions"         : [
2932       {
2933         ObjectId: 2.5.29.19 Criticality=true
2934         BasicConstraints:[
2935           CA:true
2936           PathLen: no limit
2937         ]
2938       },
2939       {
2940         ObjectId: 2.5.29.31 Criticality=false
2941         CRLDistributionPoints [
2942           [DistributionPoint:
2943              [URIName: ldap://directory.d-trust.
     net/CN=D-TRUST%20Root%20Class%203%20CA%202%20EV%
     202009,O=D-Trust%20GmbH,C=DE?
     certificaterevocationlist]
2944           , DistributionPoint:
2945              [URIName: http://www.d-trust.net/crl
     /d-trust_root_class_3_ca_2_ev_2009.crl]
2946         ]]
2947       },
2948       {
2949         ObjectId: 2.5.29.15 Criticality=true
2950         KeyUsage [
2951           Key_CertSign
2952           Crl_Sign
2953         ]
2954       },
2955       {
2956         ObjectId: 2.5.29.14 Criticality=false
2957         SubjectKeyIdentifier [
2958         KeyIdentifier [
2959         0000: D3 94 8A 4C 62 13 2A 19   2E CC AF
     72 8A 7D 36 D7  ...Lb.*....r..6.
2960         0010: 9A 1C DC 67
                                             ...g
2961         ]
```

```
2962          ]
2963        }
2964      ]},
2965    "certificate" : {
2966      "version"             : "v3",
2967      "serial number"       : "
     0BA15AFA1DDFA0B54944AFCD24A06CEC",
2968      "signature algorithm": "SHA384withECDSA",
2969      "issuer"              : "CN=DigiCert Assured
     ID Root G3, OU=www.digicert.com, O=DigiCert Inc,
     C=US",
2970      "not before"          : "2013-08-01 20:00:00.
     000 SGT",
2971      "not  after"          : "2038-01-15 20:00:00.
     000 SGT",
2972      "subject"             : "CN=DigiCert Assured
     ID Root G3, OU=www.digicert.com, O=DigiCert Inc,
     C=US",
2973      "subject public key" : "EC",
2974      "extensions"          : [
2975        {
2976          ObjectId: 2.5.29.19 Criticality=true
2977          BasicConstraints:[
2978            CA:true
2979            PathLen: no limit
2980          ]
2981        },
2982        {
2983          ObjectId: 2.5.29.15 Criticality=true
2984          KeyUsage [
2985            DigitalSignature
2986            Key_CertSign
2987            Crl_Sign
2988          ]
2989        },
2990        {
2991          ObjectId: 2.5.29.14 Criticality=false
2992          SubjectKeyIdentifier [
2993          KeyIdentifier [
2994          0000: CB D0 BD A9 E1 98 05 51   A1 4D 37
     A2 83 79 CE 8D  .......Q.M7..y..
```

```
2995         0010: 1D 2A E4 84
                                                .*..
2996         ]
2997         ]
2998       }
2999     ]},
3000   "certificate" : {
3001     "version"            : "v3",
3002     "serial number"      : "00BB401C43F55E4FB0",
3003     "signature algorithm": "SHA1withRSA",
3004     "issuer"             : "CN=SwissSign Gold CA
      - G2, O=SwissSign AG, C=CH",
3005     "not before"         : "2006-10-25 16:30:35.
     000 SGT",
3006     "not  after"         : "2036-10-25 16:30:35.
     000 SGT",
3007     "subject"            : "CN=SwissSign Gold CA
      - G2, O=SwissSign AG, C=CH",
3008     "subject public key" : "RSA",
3009     "extensions"         : [
3010       {
3011         ObjectId: 2.5.29.35 Criticality=false
3012         AuthorityKeyIdentifier [
3013         KeyIdentifier [
3014         0000: 5B 25 7B 96 A4 65 51 7E   B8 39 F3
     C0 78 66 5E E8  [%...eQ..9..xf^.
3015         0010: 3A E7 F0 EE
                                                :...
3016         ]
3017         ]
3018       },
3019       {
3020         ObjectId: 2.5.29.19 Criticality=true
3021         BasicConstraints:[
3022           CA:true
3023           PathLen: no limit
3024         ]
3025       },
3026       {
3027         ObjectId: 2.5.29.32 Criticality=false
3028         CertificatePolicies [
```

```
3029           [CertificatePolicyId: [2.16.756.1.89.1.
     2.1.1]
3030         [PolicyQualifierInfo: [
3031           qualifierID: 1.3.6.1.5.5.7.2.1
3032           qualifier: 0000: 16 20 68 74 74 70 3A
     2F   2F 72 65 70 6F 73 69 74  . http://reposit
3033         0010: 6F 72 79 2E 73 77 69 73   73 73 69
     67 6E 2E 63 6F  ory.swisssign.co
3034         0020: 6D 2F
                                                  m/
3035
3036         ]]  ]
3037         ]
3038       },
3039       {
3040         ObjectId: 2.5.29.15 Criticality=true
3041         KeyUsage [
3042           Key_CertSign
3043           Crl_Sign
3044         ]
3045       },
3046       {
3047         ObjectId: 2.5.29.14 Criticality=false
3048         SubjectKeyIdentifier [
3049         KeyIdentifier [
3050         0000: 5B 25 7B 96 A4 65 51 7E   B8 39 F3
     C0 78 66 5E E8  [%...eQ..9..xf^.
3051         0010: 3A E7 F0 EE
                                              :...
3052         ]
3053         ]
3054       }
3055     ]},
3056   "certificate" : {
3057     "version"            : "v3",
3058     "serial number"      : "
     5C8B99C55A94C5D27156DECD8980CC26",
3059     "signature algorithm": "SHA384withECDSA",
3060     "issuer"             : "CN=USERTrust ECC
     Certification Authority, O=The USERTRUST Network
     , L=Jersey City, ST=New Jersey, C=US",
```

```
3061     "not before"          : "2010-02-01 08:00:00.
     000 SGT",
3062     "not  after"          : "2038-01-19 07:59:59.
     000 SGT",
3063     "subject"             : "CN=USERTrust ECC
     Certification Authority, O=The USERTRUST Network
     , L=Jersey City, ST=New Jersey, C=US",
3064     "subject public key" : "EC",
3065     "extensions"          : [
3066       {
3067         ObjectId: 2.5.29.19 Criticality=true
3068         BasicConstraints:[
3069           CA:true
3070           PathLen: no limit
3071         ]
3072       },
3073       {
3074         ObjectId: 2.5.29.15 Criticality=true
3075         KeyUsage [
3076           Key_CertSign
3077           Crl_Sign
3078         ]
3079       },
3080       {
3081         ObjectId: 2.5.29.14 Criticality=false
3082         SubjectKeyIdentifier [
3083         KeyIdentifier [
3084         0000: 3A E1 09 86 D4 CF 19 C2   96 76 74
     49 76 DC E0 35  :........vtIv..5
3085         0010: C6 63 63 9A
                                                .cc.
3086         ]
3087         ]
3088       }
3089     ]},
3090   "certificate" : {
3091     "version"             : "v3",
3092     "serial number"       : "
     0A01428000000145 23C844B500000002",
3093     "signature algorithm": "SHA256withRSA",
3094     "issuer"              : "CN=IdenTrust
```

```
3094 Commercial Root CA 1, O=IdenTrust, C=US",
3095     "not before"         : "2014-01-17 02:12:23.
     000 SGT",
3096     "not  after"         : "2034-01-17 02:12:23.
     000 SGT",
3097     "subject"            : "CN=IdenTrust
     Commercial Root CA 1, O=IdenTrust, C=US",
3098     "subject public key" : "RSA",
3099     "extensions"         : [
3100       {
3101         ObjectId: 2.5.29.19 Criticality=true
3102         BasicConstraints:[
3103           CA:true
3104           PathLen: no limit
3105         ]
3106       },
3107       {
3108         ObjectId: 2.5.29.15 Criticality=true
3109         KeyUsage [
3110           Key_CertSign
3111           Crl_Sign
3112         ]
3113       },
3114       {
3115         ObjectId: 2.5.29.14 Criticality=false
3116         SubjectKeyIdentifier [
3117         KeyIdentifier [
3118         0000: ED 44 19 C0 D3 F0 06 8B   EE A4 7B
     BE 42 E7 26 54  .D.........B.&T
3119         0010: C8 8E 36 76
                                                ..6v
3120         ]
3121         ]
3122       }
3123     ]},
3124   "certificate" : {
3125     "version"            : "v3",
3126     "serial number"      : "
     06CEE131BE6D55C807F7C0C7FB44E620",
3127     "signature algorithm": "SHA384withRSA",
3128     "issuer"             : "CN=DigiCert CS
```

```
RSA4096 Root G5, O="DigiCert, Inc.", C=US",
    "not before"         : "2021-01-15 08:00:00.
000 SGT",
    "not  after"         : "2046-01-15 07:59:59.
000 SGT",
    "subject"            : "CN=DigiCert CS
RSA4096 Root G5, O="DigiCert, Inc.", C=US",
    "subject public key" : "RSA",
    "extensions"         : [
      {
        ObjectId: 2.5.29.19 Criticality=true
        BasicConstraints:[
          CA:true
          PathLen: no limit
        ]
      },
      {
        ObjectId: 2.5.29.15 Criticality=true
        KeyUsage [
          DigitalSignature
          Key_CertSign
          Crl_Sign
        ]
      },
      {
        ObjectId: 2.5.29.14 Criticality=false
        SubjectKeyIdentifier [
        KeyIdentifier [
        0000: 68 01 93 B1 D2 4A 40 42   69 94 46
2C 1C 5A 88 A9  h....J@Bi.F,.Z..
        0010: 25 B4 47 4F
                                            %.GO
        ]
        ]
      }
    ]},
  "certificate" : {
    "version"            : "v3",
    "serial number"      : "0509",
    "signature algorithm": "SHA1withRSA",
    "issuer"             : "CN=QuoVadis Root CA 2
```

```
3163 , O=QuoVadis Limited, C=BM",
3164     "not before"         : "2006-11-25 02:27:00.
     000 SGT",
3165     "not  after"         : "2031-11-25 02:23:33.
     000 SGT",
3166     "subject"            : "CN=QuoVadis Root CA 2
     , O=QuoVadis Limited, C=BM",
3167     "subject public key" : "RSA",
3168     "extensions"         : [
3169       {
3170         ObjectId: 2.5.29.35 Criticality=false
3171         AuthorityKeyIdentifier [
3172         KeyIdentifier [
3173         0000: 1A 84 62 BC 48 4C 33 25   04 D4 EE
     D0 F6 03 C4 19  ..b.HL3%........
3174         0010: 46 D1 94 6B
                                             F..k
3175         ]
3176         [CN=QuoVadis Root CA 2, O=QuoVadis
     Limited, C=BM]
3177         SerialNumber: [    0509]
3178         ]
3179       },
3180       {
3181         ObjectId: 2.5.29.19 Criticality=true
3182         BasicConstraints:[
3183           CA:true
3184           PathLen: no limit
3185         ]
3186       },
3187       {
3188         ObjectId: 2.5.29.15 Criticality=false
3189         KeyUsage [
3190           Key_CertSign
3191           Crl_Sign
3192         ]
3193       },
3194       {
3195         ObjectId: 2.5.29.14 Criticality=false
3196         SubjectKeyIdentifier [
3197         KeyIdentifier [
```

```
3198          0000: 1A 84 62 BC 48 4C 33 25   04 D4 EE
     D0 F6 03 C4 19  ..b.HL3%........
3199          0010: 46 D1 94 6B
                                              F..k
3200          ]
3201          ]
3202        }
3203      ]},
3204    "certificate" : {
3205      "version"            : "v3",
3206      "serial number"      : "0983F3",
3207      "signature algorithm": "SHA256withRSA",
3208      "issuer"             : "CN=D-TRUST Root Class
      3 CA 2 2009, O=D-Trust GmbH, C=DE",
3209      "not before"         : "2009-11-05 16:35:58.
     000 SGT",
3210      "not  after"         : "2029-11-05 16:35:58.
     000 SGT",
3211      "subject"            : "CN=D-TRUST Root Class
      3 CA 2 2009, O=D-Trust GmbH, C=DE",
3212      "subject public key" : "RSA",
3213      "extensions"         : [
3214        {
3215          ObjectId: 2.5.29.19 Criticality=true
3216          BasicConstraints:[
3217            CA:true
3218            PathLen: no limit
3219          ]
3220        },
3221        {
3222          ObjectId: 2.5.29.31 Criticality=false
3223          CRLDistributionPoints [
3224            [DistributionPoint:
3225               [URIName: ldap://directory.d-trust.
     net/CN=D-TRUST%20Root%20Class%203%20CA%202%202009
     ,O=D-Trust%20GmbH,C=DE?certificaterevocationlist]
3226          , DistributionPoint:
3227               [URIName: http://www.d-trust.net/crl
     /d-trust_root_class_3_ca_2_2009.crl]
3228          ]]
3229        },
```

```
3230       {
3231         ObjectId: 2.5.29.15 Criticality=true
3232         KeyUsage [
3233           Key_CertSign
3234           Crl_Sign
3235         ]
3236       },
3237       {
3238         ObjectId: 2.5.29.14 Criticality=false
3239         SubjectKeyIdentifier [
3240         KeyIdentifier [
3241         0000: FD DA 14 C4 9F 30 DE 21   BD 1E 42
     39 FC AB 63 23  .....0.!..B9..c#
3242         0010: 49 E0 F1 84
                                            I...
3243         ]
3244         ]
3245       }
3246     ]},
3247   "certificate" : {
3248     "version"            : "v3",
3249     "serial number"      : "
     78585F2EAD2C194BE3370735341328B596D46593",
3250     "signature algorithm": "SHA256withRSA",
3251     "issuer"             : "CN=QuoVadis Root CA 1
      G3, O=QuoVadis Limited, C=BM",
3252     "not before"         : "2012-01-13 01:27:44.
     000 SGT",
3253     "not  after"         : "2042-01-13 01:27:44.
     000 SGT",
3254     "subject"            : "CN=QuoVadis Root CA 1
      G3, O=QuoVadis Limited, C=BM",
3255     "subject public key" : "RSA",
3256     "extensions"         : [
3257       {
3258         ObjectId: 2.5.29.19 Criticality=true
3259         BasicConstraints:[
3260           CA:true
3261           PathLen: no limit
3262         ]
3263       },
```

```
3264        {
3265          ObjectId: 2.5.29.15 Criticality=true
3266          KeyUsage [
3267            Key_CertSign
3268            Crl_Sign
3269          ]
3270        },
3271        {
3272          ObjectId: 2.5.29.14 Criticality=false
3273          SubjectKeyIdentifier [
3274          KeyIdentifier [
3275          0000: A3 97 D6 F3 5E A2 10 E1   AB 45 9F
     3C 17 64 3C EE  ....^....E.<.d<.
3276          0010: 01 70 9C CC
                                                .p..
3277          ]
3278          ]
3279        }
3280      ]},
3281    "certificate" : {
3282      "version"            : "v3",
3283      "serial number"      : "
     01FD6D30FCA3CA51A81BBC640E35032D",
3284      "signature algorithm": "SHA384withRSA",
3285      "issuer"             : "CN=USERTrust RSA
     Certification Authority, O=The USERTRUST Network
     , L=Jersey City, ST=New Jersey, C=US",
3286      "not before"         : "2010-02-01 08:00:00.
     000 SGT",
3287      "not  after"         : "2038-01-19 07:59:59.
     000 SGT",
3288      "subject"            : "CN=USERTrust RSA
     Certification Authority, O=The USERTRUST Network
     , L=Jersey City, ST=New Jersey, C=US",
3289      "subject public key" : "RSA",
3290      "extensions"         : [
3291        {
3292          ObjectId: 2.5.29.19 Criticality=true
3293          BasicConstraints:[
3294            CA:true
3295            PathLen: no limit
```

```
3296          ]
3297        },
3298        {
3299          ObjectId: 2.5.29.15 Criticality=true
3300          KeyUsage [
3301            Key_CertSign
3302            Crl_Sign
3303          ]
3304        },
3305        {
3306          ObjectId: 2.5.29.14 Criticality=false
3307          SubjectKeyIdentifier [
3308          KeyIdentifier [
3309          0000: 53 79 BF 5A AA 2B 4A CF   54 80 E1
     D8 9B C0 9D F2  Sy.Z.+J.T.......
3310          0010: B2 03 66 CB
                                                ..f.
3311          ]
3312          ]
3313        }
3314     ]},
3315   "certificate" : {
3316     "version"            : "v3",
3317     "serial number"      : "
     18DAD19E267DE8BB4A2158CDCC6B3B4A",
3318     "signature algorithm": "SHA1withRSA",
3319     "issuer"             : "CN=VeriSign Class 3
     Public Primary Certification Authority - G5, OU
     ="(c) 2006 VeriSign, Inc. - For authorized use
     only", OU=VeriSign Trust Network, O="VeriSign,
     Inc.", C=US",
3320     "not before"         : "2006-11-08 08:00:00.
     000 SGT",
3321     "not  after"         : "2036-07-17 07:59:59.
     000 SGT",
3322     "subject"            : "CN=VeriSign Class 3
     Public Primary Certification Authority - G5, OU
     ="(c) 2006 VeriSign, Inc. - For authorized use
     only", OU=VeriSign Trust Network, O="VeriSign,
     Inc.", C=US",
3323     "subject public key" : "RSA",
```

```
3324     "extensions"          : [
3325       {
3326         ObjectId: 1.3.6.1.5.5.7.1.12 Criticality=
     false
3327       },
3328       {
3329         ObjectId: 2.5.29.19 Criticality=true
3330         BasicConstraints:[
3331           CA:true
3332           PathLen: no limit
3333         ]
3334       },
3335       {
3336         ObjectId: 2.5.29.15 Criticality=true
3337         KeyUsage [
3338           Key_CertSign
3339           Crl_Sign
3340         ]
3341       },
3342       {
3343         ObjectId: 2.5.29.14 Criticality=false
3344         SubjectKeyIdentifier [
3345         KeyIdentifier [
3346         0000: 7F D3 65 A7 C2 DD EC BB   F0 30 09
     F3 43 39 FA 02  ..e......0..C9..
3347         0010: AF 33 31 33
                                            .313
3348         ]
3349         ]
3350       }
3351     ]},
3352   "certificate" : {
3353     "version"             : "v3",
3354     "serial number"       : "05C6",
3355     "signature algorithm": "SHA1withRSA",
3356     "issuer"              : "CN=QuoVadis Root CA 3
     , O=QuoVadis Limited, C=BM",
3357     "not before"          : "2006-11-25 03:11:23.
     000 SGT",
3358     "not  after"          : "2031-11-25 03:06:44.
     000 SGT",
```

```
3359     "subject"            : "CN=QuoVadis Root CA 3
     , O=QuoVadis Limited, C=BM",
3360     "subject public key" : "RSA",
3361     "extensions"         : [
3362       {
3363         ObjectId: 2.5.29.35 Criticality=false
3364         AuthorityKeyIdentifier [
3365         KeyIdentifier [
3366         0000: F2 C0 13 E0 82 43 3E FB   EE 2F 67
     32 96 35 5C DB  .....C>../g2.5\.
3367         0010: B8 CB 02 D0
                                             ....
3368         ]
3369         [CN=QuoVadis Root CA 3, O=QuoVadis
     Limited, C=BM]
3370         SerialNumber: [    05c6]
3371         ]
3372       },
3373       {
3374         ObjectId: 2.5.29.19 Criticality=true
3375         BasicConstraints:[
3376           CA:true
3377           PathLen: no limit
3378         ]
3379       },
3380       {
3381         ObjectId: 2.5.29.32 Criticality=false
3382         CertificatePolicies [
3383           [CertificatePolicyId: [1.3.6.1.4.1.8024
     .0.3]
3384         [PolicyQualifierInfo: [
3385           qualifierID: 1.3.6.1.5.5.7.2.2
3386           qualifier: 0000: 30 81 86 1A 81 83 41
     6E   79 20 75 73 65 20 6F 66  0.....Any use of
3387         0010: 20 74 68 69 73 20 43 65   72 74 69
     66 69 63 61 74   this Certificat
3388         0020: 65 20 63 6F 6E 73 74 69   74 75 74
     65 73 20 61 63  e constitutes ac
3389         0030: 63 65 70 74 61 6E 63 65   20 6F 66
     20 74 68 65 20  ceptance of the
3390         0040: 51 75 6F 56 61 64 69 73   20 52 6F
```

```
3390 6F 74 20 43 41  QuoVadis Root CA
3391         0050: 20 33 20 43 65 72 74 69   66 69 63
     61 74 65 20 50   3 Certificate P
3392         0060: 6F 6C 69 63 79 20 2F 20   43 65 72
     74 69 66 69 63  olicy / Certific
3393         0070: 61 74 69 6F 6E 20 50 72   61 63 74
     69 63 65 20 53  ation Practice S
3394         0080: 74 61 74 65 6D 65 6E 74   2E
                           tatement.
3395
3396         ], PolicyQualifierInfo: [
3397           qualifierID: 1.3.6.1.5.5.7.2.1
3398           qualifier: 0000: 16 21 68 74 74 70 3A
     2F   2F 77 77 77 2E 71 75 6F  .!http://www.quo
3399         0010: 76 61 64 69 73 67 6C 6F   62 61 6C
     2E 63 6F 6D 2F  vadisglobal.com/
3400         0020: 63 70 73
                                                cps
3401
3402         ]]  ]
3403         ]
3404       },
3405       {
3406         ObjectId: 2.5.29.15 Criticality=false
3407         KeyUsage [
3408           Key_CertSign
3409           Crl_Sign
3410         ]
3411       },
3412       {
3413         ObjectId: 2.5.29.14 Criticality=false
3414         SubjectKeyIdentifier [
3415         KeyIdentifier [
3416         0000: F2 C0 13 E0 82 43 3E FB   EE 2F 67
     32 96 35 5C DB  .....C>../g2.5\.
3417         0010: B8 CB 02 D0
                                              ....
3418         ]
3419         ]
3420       }
3421     ]},
```

```
3422   "certificate" : {
3423     "version"            : "v3",
3424     "serial number"      : "00",
3425     "signature algorithm": "SHA256withRSA",
3426     "issuer"             : "CN=Starfield Services
      Root Certificate Authority - G2, O="Starfield
     Technologies, Inc.", L=Scottsdale, ST=Arizona, C=
     US",
3427     "not before"         : "2009-09-01 08:00:00.
     000 SGT",
3428     "not  after"         : "2038-01-01 07:59:59.
     000 SGT",
3429     "subject"            : "CN=Starfield Services
      Root Certificate Authority - G2, O="Starfield
     Technologies, Inc.", L=Scottsdale, ST=Arizona, C=
     US",
3430     "subject public key" : "RSA",
3431     "extensions"         : [
3432       {
3433         ObjectId: 2.5.29.19 Criticality=true
3434         BasicConstraints:[
3435           CA:true
3436           PathLen: no limit
3437         ]
3438       },
3439       {
3440         ObjectId: 2.5.29.15 Criticality=true
3441         KeyUsage [
3442           Key_CertSign
3443           Crl_Sign
3444         ]
3445       },
3446       {
3447         ObjectId: 2.5.29.14 Criticality=false
3448         SubjectKeyIdentifier [
3449         KeyIdentifier [
3450         0000: 9C 5F 00 DF AA 01 D7 30   2B 38 88
     A2 B8 6D 4A 9C  ._.....0+8...mJ.
3451         0010: F2 11 91 83
                                                ....
3452         ]
```

```
3453          ]
3454        }
3455      ]},
3456    "certificate" : {
3457      "version"             : "v3",
3458      "serial number"       : "
     066C9FD5749736663F3B0B9AD9E89E7603F24A",
3459      "signature algorithm": "SHA256withECDSA",
3460      "issuer"              : "CN=Amazon Root CA 3,
     O=Amazon, C=US",
3461      "not before"          : "2015-05-26 08:00:00.
     000 SGT",
3462      "not  after"          : "2040-05-26 08:00:00.
     000 SGT",
3463      "subject"             : "CN=Amazon Root CA 3,
     O=Amazon, C=US",
3464      "subject public key" : "EC",
3465      "extensions"          : [
3466        {
3467          ObjectId: 2.5.29.19 Criticality=true
3468          BasicConstraints:[
3469            CA:true
3470            PathLen: no limit
3471          ]
3472        },
3473        {
3474          ObjectId: 2.5.29.15 Criticality=true
3475          KeyUsage [
3476            DigitalSignature
3477            Key_CertSign
3478            Crl_Sign
3479          ]
3480        },
3481        {
3482          ObjectId: 2.5.29.14 Criticality=false
3483          SubjectKeyIdentifier [
3484          KeyIdentifier [
3485          0000: AB B6 DB D7 06 9E 37 AC   30 86 07
     91 70 C7 9C C4  ......7.0...p...
3486          0010: 19 B1 78 C0
                                              ..x.
```

```
3487          ]
3488          ]
3489        }
3490      ]},
3491    "certificate" : {
3492      "version"            : "v3",
3493      "serial number"      : "
      1ED397095FD8B4B347701EAABE7F45B3",
3494      "signature algorithm": "SHA384withRSA",
3495      "issuer"             : "CN=Microsoft RSA Root
       Certificate Authority 2017, O=Microsoft
      Corporation, C=US",
3496      "not before"         : "2019-12-19 06:51:22.
      000 SGT",
3497      "not  after"         : "2042-07-19 07:00:23.
      000 SGT",
3498      "subject"            : "CN=Microsoft RSA Root
       Certificate Authority 2017, O=Microsoft
      Corporation, C=US",
3499      "subject public key" : "RSA",
3500      "extensions"         : [
3501        {
3502          ObjectId: 1.3.6.1.4.1.311.21.1
      Criticality=false
3503        },
3504        {
3505          ObjectId: 2.5.29.19 Criticality=true
3506          BasicConstraints:[
3507            CA:true
3508            PathLen: no limit
3509          ]
3510        },
3511        {
3512          ObjectId: 2.5.29.15 Criticality=true
3513          KeyUsage [
3514            DigitalSignature
3515            Key_CertSign
3516            Crl_Sign
3517          ]
3518        },
3519        {
```

```
3520         ObjectId: 2.5.29.14 Criticality=false
3521         SubjectKeyIdentifier [
3522         KeyIdentifier [
3523         0000: 09 CB 59 7F 86 B2 70 8F   1A C3 39
     E3 C0 D9 E9 BF  ..Y...p...9.....
3524         0010: BB 4D B2 23
                                                .M.#
3525         ]
3526         ]
3527       }
3528     ]},
3529   "certificate" : {
3530     "version"            : "v3",
3531     "serial number"      : "
     2EF59B0228A7DB7AFFD5A3A9EEBD03A0CF126A1D",
3532     "signature algorithm": "SHA256withRSA",
3533     "issuer"             : "CN=QuoVadis Root CA 3
      G3, O=QuoVadis Limited, C=BM",
3534     "not before"         : "2012-01-13 04:26:32.
     000 SGT",
3535     "not  after"         : "2042-01-13 04:26:32.
     000 SGT",
3536     "subject"            : "CN=QuoVadis Root CA 3
      G3, O=QuoVadis Limited, C=BM",
3537     "subject public key" : "RSA",
3538     "extensions"         : [
3539       {
3540         ObjectId: 2.5.29.19 Criticality=true
3541         BasicConstraints:[
3542           CA:true
3543           PathLen: no limit
3544         ]
3545       },
3546       {
3547         ObjectId: 2.5.29.15 Criticality=true
3548         KeyUsage [
3549           Key_CertSign
3550           Crl_Sign
3551         ]
3552       },
3553       {
```

```
3554          ObjectId: 2.5.29.14 Criticality=false
3555          SubjectKeyIdentifier [
3556          KeyIdentifier [
3557          0000: C6 17 D0 BC A8 EA 02 43   F2 1B 06
     99 5D 2B 90 20  .......C....]+.
3558          0010: B9 D7 9C E4
                                              ....
3559          ]
3560          ]
3561        }
3562      ]},
3563    "certificate" : {
3564      "version"            : "v3",
3565      "serial number"      : "570A119742C4E3CC",
3566      "signature algorithm": "SHA256withRSA",
3567      "issuer"             : "CN=Actalis
     Authentication Root CA, O=Actalis S.p.A./
     03358520967, L=Milan, C=IT",
3568      "not before"         : "2011-09-22 19:22:02.
     000 SGT",
3569      "not  after"         : "2030-09-22 19:22:02.
     000 SGT",
3570      "subject"            : "CN=Actalis
     Authentication Root CA, O=Actalis S.p.A./
     03358520967, L=Milan, C=IT",
3571      "subject public key" : "RSA",
3572      "extensions"         : [
3573        {
3574          ObjectId: 2.5.29.35 Criticality=false
3575          AuthorityKeyIdentifier [
3576          KeyIdentifier [
3577          0000: 52 D8 88 3A C8 9F 78 66   ED 89 F3
     7B 38 70 94 C9  R..:..xf....8p..
3578          0010: 02 02 36 D0
                                              ..6.
3579          ]
3580          ]
3581        },
3582        {
3583          ObjectId: 2.5.29.19 Criticality=true
3584          BasicConstraints:[
```

```
3585           CA:true
3586           PathLen: no limit
3587         ]
3588       },
3589       {
3590         ObjectId: 2.5.29.15 Criticality=true
3591         KeyUsage [
3592           Key_CertSign
3593           Crl_Sign
3594         ]
3595       },
3596       {
3597         ObjectId: 2.5.29.14 Criticality=false
3598         SubjectKeyIdentifier [
3599         KeyIdentifier [
3600         0000: 52 D8 88 3A C8 9F 78 66   ED 89 F3
     7B 38 70 94 C9  R..:..xf....8p..
3601         0010: 02 02 36 D0
                                                ..6.
3602         ]
3603         ]
3604       }
3605     ]},
3606   "certificate" : {
3607     "version"            : "v3",
3608     "serial number"      : "
     03698FE712D519F3CED0FDB7B1643011",
3609     "signature algorithm": "SHA384withECDSA",
3610     "issuer"             : "CN=DigiCert CS ECC
     P384 Root G5, O="DigiCert, Inc.", C=US",
3611     "not before"         : "2021-01-15 08:00:00.
     000 SGT",
3612     "not  after"         : "2046-01-15 07:59:59.
     000 SGT",
3613     "subject"            : "CN=DigiCert CS ECC
     P384 Root G5, O="DigiCert, Inc.", C=US",
3614     "subject public key" : "EC",
3615     "extensions"         : [
3616       {
3617         ObjectId: 2.5.29.19 Criticality=true
3618         BasicConstraints:[
```

```
3619           CA:true
3620           PathLen: no limit
3621         ]
3622       },
3623       {
3624         ObjectId: 2.5.29.15 Criticality=true
3625         KeyUsage [
3626           DigitalSignature
3627           Key_CertSign
3628           Crl_Sign
3629         ]
3630       },
3631       {
3632         ObjectId: 2.5.29.14 Criticality=false
3633         SubjectKeyIdentifier [
3634         KeyIdentifier [
3635         0000: F0 8C 98 71 39 38 65 C2   3A 1B A6
     17 66 1D C8 ED  ...q98e.:...f...
3636         0010: 65 DE 92 36
                                                e..6
3637         ]
3638         ]
3639       }
3640     ]},
3641   "certificate" : {
3642     "version"            : "v3",
3643     "serial number"      : "00FEDCE3010FC948FF",
3644     "signature algorithm": "SHA1withRSA",
3645     "issuer"             : "CN=Certigna, O=
     Dhimyotis, C=FR",
3646     "not before"         : "2007-06-29 23:13:05.
     000 SGT",
3647     "not  after"         : "2027-06-29 23:13:05.
     000 SGT",
3648     "subject"            : "CN=Certigna, O=
     Dhimyotis, C=FR",
3649     "subject public key" : "RSA",
3650     "extensions"         : [
3651       {
3652         ObjectId: 2.5.29.35 Criticality=false
3653         AuthorityKeyIdentifier [
```

```
3654         KeyIdentifier [
3655         0000: 1A ED FE 41 39 90 B4 24   59 BE 01
     F2 52 D5 45 F6  ...A9..$Y...R.E.
3656         0010: 5A 39 DC 11
                                            Z9..
3657         ]
3658         [CN=Certigna, O=Dhimyotis, C=FR]
3659         SerialNumber: [    fedce301 0fc948ff]
3660         ]
3661       },
3662       {
3663         ObjectId: 2.5.29.19 Criticality=true
3664         BasicConstraints:[
3665           CA:true
3666           PathLen: no limit
3667         ]
3668       },
3669       {
3670         ObjectId: 2.5.29.15 Criticality=true
3671         KeyUsage [
3672           Key_CertSign
3673           Crl_Sign
3674         ]
3675       },
3676       {
3677         ObjectId: 2.16.840.1.113730.1.1
     Criticality=false
3678         NetscapeCertType [
3679            SSL CA
3680            S/MIME CA
3681            Object Signing CA]
3682       },
3683       {
3684         ObjectId: 2.5.29.14 Criticality=false
3685         SubjectKeyIdentifier [
3686         KeyIdentifier [
3687         0000: 1A ED FE 41 39 90 B4 24   59 BE 01
     F2 52 D5 45 F6  ...A9..$Y...R.E.
3688         0010: 5A 39 DC 11
                                            Z9..
3689         ]
```

```
3690          ]
3691        }
3692      ]},
3693    "certificate" : {
3694      "version"            : "v3",
3695      "serial number"      : "
     0203E5AEC58D04251AAB1125AA",
3696      "signature algorithm": "SHA384withRSA",
3697      "issuer"             : "CN=GTS Root R2, O=
     Google Trust Services LLC, C=US",
3698      "not before"         : "2016-06-22 08:00:00.
     000 SGT",
3699      "not  after"         : "2036-06-22 08:00:00.
     000 SGT",
3700      "subject"            : "CN=GTS Root R2, O=
     Google Trust Services LLC, C=US",
3701      "subject public key" : "RSA",
3702      "extensions"         : [
3703        {
3704          ObjectId: 2.5.29.19 Criticality=true
3705          BasicConstraints:[
3706            CA:true
3707            PathLen: no limit
3708          ]
3709        },
3710        {
3711          ObjectId: 2.5.29.15 Criticality=true
3712          KeyUsage [
3713            DigitalSignature
3714            Key_CertSign
3715            Crl_Sign
3716          ]
3717        },
3718        {
3719          ObjectId: 2.5.29.14 Criticality=false
3720          SubjectKeyIdentifier [
3721          KeyIdentifier [
3722          0000: BB FF CA 8E 23 9F 4F 99   CA DB E2
     68 A6 A5 15 27  ....#.O....h...'
3723          0010: 17 1E D9 0E
                                              ....
```

```
3724         ]
3725         ]
3726       }
3727     ]},
3728   "certificate" : {
3729     "version"            : "v3",
3730     "serial number"      : "3AB6508B",
3731     "signature algorithm": "SHA1withRSA",
3732     "issuer"             : "CN=QuoVadis Root
     Certification Authority, OU=Root Certification
     Authority, O=QuoVadis Limited, C=BM",
3733     "not before"         : "2001-03-20 02:33:33.
     000 SGT",
3734     "not  after"         : "2021-03-18 02:33:33.
     000 SGT",
3735     "subject"            : "CN=QuoVadis Root
     Certification Authority, OU=Root Certification
     Authority, O=QuoVadis Limited, C=BM",
3736     "subject public key" : "RSA",
3737     "extensions"         : [
3738       {
3739         ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=
     false
3740         AuthorityInfoAccess [
3741           [
3742            accessMethod: ocsp
3743            accessLocation: URIName: https://ocsp.
     quovadisoffshore.com
3744         ]
3745         ]
3746       },
3747       {
3748         ObjectId: 2.5.29.35 Criticality=false
3749         AuthorityKeyIdentifier [
3750         KeyIdentifier [
3751         0000: 8B 4B 6D ED D3 29 B9 06   19 EC 39
     39 A9 F0 97 84  .Km..)....99....
3752         0010: 6A CB EF DF
                                             j...
3753         ]
3754         [CN=QuoVadis Root Certification Authority
```

```
3754 , OU=Root Certification Authority, O=QuoVadis
     Limited, C=BM]
3755         SerialNumber: [    3ab6508b]
3756         ]
3757       },
3758       {
3759         ObjectId: 2.5.29.19 Criticality=true
3760         BasicConstraints:[
3761           CA:true
3762           PathLen: no limit
3763         ]
3764       },
3765       {
3766         ObjectId: 2.5.29.32 Criticality=false
3767         CertificatePolicies [
3768           [CertificatePolicyId: [1.3.6.1.4.1.8024
     .0.1]
3769         [PolicyQualifierInfo: [
3770           qualifierID: 1.3.6.1.5.5.7.2.2
3771           qualifier: 0000: 30 81 C7 1A 81 C4 52
     65   6C 69 61 6E 63 65 20 6F  0.....Reliance o
3772         0010: 6E 20 74 68 65 20 51 75   6F 56 61
     64 69 73 20 52  n the QuoVadis R
3773         0020: 6F 6F 74 20 43 65 72 74   69 66 69
     63 61 74 65 20  oot Certificate
3774         0030: 62 79 20 61 6E 79 20 70   61 72 74
     79 20 61 73 73  by any party ass
3775         0040: 75 6D 65 73 20 61 63 63   65 70 74
     61 6E 63 65 20  umes acceptance
3776         0050: 6F 66 20 74 68 65 20 74   68 65 6E
     20 61 70 70 6C  of the then appl
3777         0060: 69 63 61 62 6C 65 20 73   74 61 6E
     64 61 72 64 20  icable standard
3778         0070: 74 65 72 6D 73 20 61 6E   64 20 63
     6F 6E 64 69 74  terms and condit
3779         0080: 69 6F 6E 73 20 6F 66 20   75 73 65
     2C 20 63 65 72  ions of use, cer
3780         0090: 74 69 66 69 63 61 74 69   6F 6E 20
     70 72 61 63 74  tification pract
3781         00A0: 69 63 65 73 2C 20 61 6E   64 20 74
     68 65 20 51 75  ices, and the Qu
```

```
3782          00B0: 6F 56 61 64 69 73 20 43   65 72 74
     69 66 69 63 61  oVadis Certifica
3783          00C0: 74 65 20 50 6F 6C 69 63   79 2E
                        te Policy.
3784
3785          ], PolicyQualifierInfo: [
3786            qualifierID: 1.3.6.1.5.5.7.2.1
3787            qualifier: 0000: 16 16 68 74 74 70 3A
     2F   2F 77 77 77 2E 71 75 6F  ..http://www.quo
3788          0010: 76 61 64 69 73 2E 62 6D
                                  vadis.bm
3789
3790          ]]  ]
3791          ]
3792        },
3793        {
3794          ObjectId: 2.5.29.15 Criticality=true
3795          KeyUsage [
3796            Key_CertSign
3797            Crl_Sign
3798          ]
3799        },
3800        {
3801          ObjectId: 2.5.29.14 Criticality=false
3802          SubjectKeyIdentifier [
3803          KeyIdentifier [
3804          0000: 8B 4B 6D ED D3 29 B9 06   19 EC 39
     39 A9 F0 97 84  .Km..)....99....
3805          0010: 6A CB EF DF
                                            j...
3806          ]
3807          ]
3808        }
3809      ]},
3810    "certificate" : {
3811      "version"            : "v3",
3812      "serial number"      : "02",
3813      "signature algorithm": "SHA256withRSA",
3814      "issuer"             : "CN=Buypass Class 3
     Root CA, O=Buypass AS-983163327, C=NO",
3815      "not before"         : "2010-10-26 16:28:58.
```

```
3815 000 SGT",
3816     "not  after"         : "2040-10-26 16:28:58.
     000 SGT",
3817     "subject"            : "CN=Buypass Class 3
     Root CA, O=Buypass AS-983163327, C=NO",
3818     "subject public key" : "RSA",
3819     "extensions"         : [
3820       {
3821         ObjectId: 2.5.29.19 Criticality=true
3822         BasicConstraints:[
3823           CA:true
3824           PathLen: no limit
3825         ]
3826       },
3827       {
3828         ObjectId: 2.5.29.15 Criticality=true
3829         KeyUsage [
3830           Key_CertSign
3831           Crl_Sign
3832         ]
3833       },
3834       {
3835         ObjectId: 2.5.29.14 Criticality=false
3836         SubjectKeyIdentifier [
3837         KeyIdentifier [
3838         0000: 47 B8 CD FF E5 6F EE F8   B2 EC 2F
     4E 0E F9 25 B0  G....o..../N..%.
3839         0010: 8E 3C 6B C3
                                                .<k.
3840         ]
3841         ]
3842       }
3843     ]},
3844   "certificate" : {
3845     "version"            : "v3",
3846     "serial number"      : "
     35FC265CD9844FC93D263D579BAED756",
3847     "signature algorithm": "SHA384withECDSA",
3848     "issuer"             : "CN=thawte Primary
     Root CA - G2, OU="(c) 2007 thawte, Inc. - For
     authorized use only", O="thawte, Inc.", C=US",
```

```
3849     "not before"          : "2007-11-05 08:00:00.
     000 SGT",
3850     "not  after"          : "2038-01-19 07:59:59.
     000 SGT",
3851     "subject"             : "CN=thawte Primary
     Root CA - G2, OU="(c) 2007 thawte, Inc. - For
     authorized use only", O="thawte, Inc.", C=US",
3852     "subject public key" : "EC",
3853     "extensions"          : [
3854       {
3855         ObjectId: 2.5.29.19 Criticality=true
3856         BasicConstraints:[
3857           CA:true
3858           PathLen: no limit
3859         ]
3860       },
3861       {
3862         ObjectId: 2.5.29.15 Criticality=true
3863         KeyUsage [
3864           Key_CertSign
3865           Crl_Sign
3866         ]
3867       },
3868       {
3869         ObjectId: 2.5.29.14 Criticality=false
3870         SubjectKeyIdentifier [
3871         KeyIdentifier [
3872         0000: 9A D8 00 30 00 E7 6B 7F   85 18 EE
     8B B6 CE 8A 0C  ...0..k.........
3873         0010: F8 11 E1 BB
                                                ....
3874         ]
3875         ]
3876       }
3877     ]},
3878   "certificate" : {
3879     "version"             : "v3",
3880     "serial number"       : "
     41D29DD172EAEEA780C12C6CE92F8752",
3881     "signature algorithm": "SHA384withECDSA",
3882     "issuer"              : "CN=ISRG Root X2, O=
```

```
3882 Internet Security Research Group, C=US",
3883     "not before"         : "2020-09-04 08:00:00.
     000 SGT",
3884     "not  after"         : "2040-09-18 24:00:00.
     000 SGT",
3885     "subject"            : "CN=ISRG Root X2, O=
     Internet Security Research Group, C=US",
3886     "subject public key" : "EC",
3887     "extensions"         : [
3888       {
3889         ObjectId: 2.5.29.19 Criticality=true
3890         BasicConstraints:[
3891           CA:true
3892           PathLen: no limit
3893         ]
3894       },
3895       {
3896         ObjectId: 2.5.29.15 Criticality=true
3897         KeyUsage [
3898           Key_CertSign
3899           Crl_Sign
3900         ]
3901       },
3902       {
3903         ObjectId: 2.5.29.14 Criticality=false
3904         SubjectKeyIdentifier [
3905         KeyIdentifier [
3906         0000: 7C 42 96 AE DE 4B 48 3B   FA 92 F8
     9E 8C CF 6D 8B  .B...KH;......m.
3907         0010: A9 72 37 95
                                                .r7.
3908         ]
3909         ]
3910       }
3911     ]},
3912   "certificate" : {
3913     "version"            : "v3",
3914     "serial number"      : "
     401AC46421B31321030EBBE4121AC51D",
3915     "signature algorithm": "SHA256withRSA",
3916     "issuer"             : "CN=VeriSign Universal
```

```
3916  Root Certification Authority, OU="(c) 2008
     VeriSign, Inc. - For authorized use only", OU=
     VeriSign Trust Network, O="VeriSign, Inc.", C=US
     ",
3917     "not before"         : "2008-04-02 08:00:00.
     000 SGT",
3918     "not  after"         : "2037-12-02 07:59:59.
     000 SGT",
3919     "subject"            : "CN=VeriSign Universal
      Root Certification Authority, OU="(c) 2008
     VeriSign, Inc. - For authorized use only", OU=
     VeriSign Trust Network, O="VeriSign, Inc.", C=US
     ",
3920     "subject public key" : "RSA",
3921     "extensions"         : [
3922       {
3923         ObjectId: 1.3.6.1.5.5.7.1.12 Criticality=
     false
3924       },
3925       {
3926         ObjectId: 2.5.29.19 Criticality=true
3927         BasicConstraints:[
3928           CA:true
3929           PathLen: no limit
3930         ]
3931       },
3932       {
3933         ObjectId: 2.5.29.15 Criticality=true
3934         KeyUsage [
3935           Key_CertSign
3936           Crl_Sign
3937         ]
3938       },
3939       {
3940         ObjectId: 2.5.29.14 Criticality=false
3941         SubjectKeyIdentifier [
3942         KeyIdentifier [
3943         0000: B6 77 FA 69 48 47 9F 53   12 D5 C2
     EA 07 32 76 07  .w.iHG.S.....2v.
3944         0010: D1 97 07 19
                                             ....
```

```
3945          ]
3946          ]
3947        }
3948      ]},
3949    "certificate" : {
3950      "version"            : "v3",
3951      "serial number"      : "
     066C9FCF99BF8C0A39E2F0788A43E696365BCA",
3952      "signature algorithm": "SHA256withRSA",
3953      "issuer"             : "CN=Amazon Root CA 1,
     O=Amazon, C=US",
3954      "not before"         : "2015-05-26 08:00:00.
     000 SGT",
3955      "not  after"         : "2038-01-17 08:00:00.
     000 SGT",
3956      "subject"            : "CN=Amazon Root CA 1,
     O=Amazon, C=US",
3957      "subject public key" : "RSA",
3958      "extensions"         : [
3959        {
3960          ObjectId: 2.5.29.19 Criticality=true
3961          BasicConstraints:[
3962            CA:true
3963            PathLen: no limit
3964          ]
3965        },
3966        {
3967          ObjectId: 2.5.29.15 Criticality=true
3968          KeyUsage [
3969            DigitalSignature
3970            Key_CertSign
3971            Crl_Sign
3972          ]
3973        },
3974        {
3975          ObjectId: 2.5.29.14 Criticality=false
3976          SubjectKeyIdentifier [
3977          KeyIdentifier [
3978          0000: 84 18 CC 85 34 EC BC 0C   94 94 2E
     08 59 9C C7 B2  ....4.......Y...
3979          0010: 10 4E 0A 08
```

```
3979                                                .N..
3980         ]
3981         ]
3982       }
3983     ]},
3984   "certificate" : {
3985     "version"            : "v3",
3986     "serial number"      : "
     066C9FD29635869F0A0FE58678F85B26BB8A37",
3987     "signature algorithm": "SHA384withRSA",
3988     "issuer"             : "CN=Amazon Root CA 2,
     O=Amazon, C=US",
3989     "not before"         : "2015-05-26 08:00:00.
     000 SGT",
3990     "not  after"         : "2040-05-26 08:00:00.
     000 SGT",
3991     "subject"            : "CN=Amazon Root CA 2,
     O=Amazon, C=US",
3992     "subject public key" : "RSA",
3993     "extensions"         : [
3994       {
3995         ObjectId: 2.5.29.19 Criticality=true
3996         BasicConstraints:[
3997           CA:true
3998           PathLen: no limit
3999         ]
4000       },
4001       {
4002         ObjectId: 2.5.29.15 Criticality=true
4003         KeyUsage [
4004           DigitalSignature
4005           Key_CertSign
4006           Crl_Sign
4007         ]
4008       },
4009       {
4010         ObjectId: 2.5.29.14 Criticality=false
4011         SubjectKeyIdentifier [
4012         KeyIdentifier [
4013         0000: B0 0C F0 4C 30 F4 05 58   02 48 FD
     33 E5 52 AF 4B  ...L0..X.H.3.R.K
```

```
4014          0010: 84 E3 66 52
                                                ..fR
4015          ]
4016          ]
4017        }
4018      ]},
4019    "certificate" : {
4020      "version"            : "v3",
4021      "serial number"      : "
     2A38A41C960A04DE42B228A50BE8349802",
4022      "signature algorithm": "SHA256withECDSA",
4023      "issuer"             : "CN=GlobalSign, O=
     GlobalSign, OU=GlobalSign ECC Root CA - R4",
4024      "not before"         : "2012-11-13 08:00:00.
     000 SGT",
4025      "not  after"         : "2038-01-19 11:14:07.
     000 SGT",
4026      "subject"            : "CN=GlobalSign, O=
     GlobalSign, OU=GlobalSign ECC Root CA - R4",
4027      "subject public key" : "EC",
4028      "extensions"         : [
4029        {
4030          ObjectId: 2.5.29.19 Criticality=true
4031          BasicConstraints:[
4032            CA:true
4033            PathLen: no limit
4034          ]
4035        },
4036        {
4037          ObjectId: 2.5.29.15 Criticality=true
4038          KeyUsage [
4039            Key_CertSign
4040            Crl_Sign
4041          ]
4042        },
4043        {
4044          ObjectId: 2.5.29.14 Criticality=false
4045          SubjectKeyIdentifier [
4046          KeyIdentifier [
4047          0000: 54 B0 7B AD 45 B8 E2 40   7F FB 0A
     6E FB BE 33 C9  T...E..@...n..3.
```

```
4048         0010: 3C A3 84 D5                                        <...
4049         ]
4050         ]
4051       }
4052     ]},
4053   "certificate" : {
4054     "version"            : "v3",
4055     "serial number"      : "00C9CDD3E9D57D23CE",
4056     "signature algorithm": "SHA1withRSA",
4057     "issuer"             : "CN=Global Chambersign
      Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=
     A82743287, L=Madrid (see current address at www.
     camerfirma.com/address), C=EU",
4058     "not before"         : "2008-08-01 20:31:40.
     000 SGT",
4059     "not  after"         : "2038-07-31 20:31:40.
     000 SGT",
4060     "subject"            : "CN=Global Chambersign
      Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=
     A82743287, L=Madrid (see current address at www.
     camerfirma.com/address), C=EU",
4061     "subject public key" : "RSA",
4062     "extensions"         : [
4063       {
4064         ObjectId: 2.5.29.35 Criticality=false
4065         AuthorityKeyIdentifier [
4066         KeyIdentifier [
4067         0000: B9 09 CA 9C 1E DB D3 6C   3A 6B AE
     ED 54 F1 5B 93  .......l:k..T.[.
4068         0010: 06 35 2E 5E                                        .5.^
4069         ]
4070         [CN=Global Chambersign Root - 2008, O=AC
     Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid
      (see current address at www.camerfirma.com/
     address), C=EU]
4071         SerialNumber: [    c9cdd3e9 d57d23ce]
4072         ]
4073       },
4074       {
```

```
4075         ObjectId: 2.5.29.19 Criticality=true
4076         BasicConstraints:[
4077           CA:true
4078           PathLen:12
4079         ]
4080       },
4081       {
4082         ObjectId: 2.5.29.32 Criticality=false
4083         CertificatePolicies [
4084           [CertificatePolicyId: [2.5.29.32.0]
4085         [PolicyQualifierInfo: [
4086           qualifierID: 1.3.6.1.5.5.7.2.1
4087           qualifier: 0000: 16 1C 68 74 74 70 3A
     2F   2F 70 6F 6C 69 63 79 2E  ..http://policy.
4088         0010: 63 61 6D 65 72 66 69 72   6D 61 2E
     63 6F 6D        camerfirma.com
4089
4090         ]]  ]
4091         ]
4092       },
4093       {
4094         ObjectId: 2.5.29.15 Criticality=true
4095         KeyUsage [
4096           Key_CertSign
4097           Crl_Sign
4098         ]
4099       },
4100       {
4101         ObjectId: 2.5.29.14 Criticality=false
4102         SubjectKeyIdentifier [
4103         KeyIdentifier [
4104         0000: B9 09 CA 9C 1E DB D3 6C   3A 6B AE
     ED 54 F1 5B 93  .......l:k..T.[.
4105         0010: 06 35 2E 5E
                                                .5.^
4106         ]
4107         ]
4108       }
4109     ]},
4110   "certificate" : {
4111     "version"            : "v3",
```

```
4112     "serial number"      : "
     600197B746A7EAB4B49AD64B2FF790FB",
4113     "signature algorithm": "SHA256withRSA",
4114     "issuer"             : "CN=thawte Primary
     Root CA - G3, OU="(c) 2008 thawte, Inc. - For
     authorized use only", OU=Certification Services
     Division, O="thawte, Inc.", C=US",
4115     "not before"         : "2008-04-02 08:00:00.
     000 SGT",
4116     "not  after"         : "2037-12-02 07:59:59.
     000 SGT",
4117     "subject"            : "CN=thawte Primary
     Root CA - G3, OU="(c) 2008 thawte, Inc. - For
     authorized use only", OU=Certification Services
     Division, O="thawte, Inc.", C=US",
4118     "subject public key" : "RSA",
4119     "extensions"         : [
4120       {
4121         ObjectId: 2.5.29.19 Criticality=true
4122         BasicConstraints:[
4123           CA:true
4124           PathLen: no limit
4125         ]
4126       },
4127       {
4128         ObjectId: 2.5.29.15 Criticality=true
4129         KeyUsage [
4130           Key_CertSign
4131           Crl_Sign
4132         ]
4133       },
4134       {
4135         ObjectId: 2.5.29.14 Criticality=false
4136         SubjectKeyIdentifier [
4137         KeyIdentifier [
4138         0000: AD 6C AA 94 60 9C ED E4   FF FA 3E
     0A 74 2B 63 03  .l..`.....>.t+c.
4139         0010: F7 B6 59 BF
                                                ..Y.
4140         ]
4141         ]
```

```
4142       }
4143     ]},
4144   "certificate" : {
4145     "version"            : "v3",
4146     "serial number"      : "
     4CAAF9CADB636FE01FF74ED85B03869D",
4147     "signature algorithm": "SHA384withRSA",
4148     "issuer"             : "CN=COMODO RSA
     Certification Authority, O=COMODO CA Limited, L=
     Salford, ST=Greater Manchester, C=GB",
4149     "not before"         : "2010-01-19 08:00:00.
     000 SGT",
4150     "not  after"         : "2038-01-19 07:59:59.
     000 SGT",
4151     "subject"            : "CN=COMODO RSA
     Certification Authority, O=COMODO CA Limited, L=
     Salford, ST=Greater Manchester, C=GB",
4152     "subject public key" : "RSA",
4153     "extensions"         : [
4154       {
4155         ObjectId: 2.5.29.19 Criticality=true
4156         BasicConstraints:[
4157           CA:true
4158           PathLen: no limit
4159         ]
4160       },
4161       {
4162         ObjectId: 2.5.29.15 Criticality=true
4163         KeyUsage [
4164           Key_CertSign
4165           Crl_Sign
4166         ]
4167       },
4168       {
4169         ObjectId: 2.5.29.14 Criticality=false
4170         SubjectKeyIdentifier [
4171         KeyIdentifier [
4172         0000: BB AF 7E 02 3D FA A6 F1   3C 84 8E
     AD EE 38 98 EC  ....=...<....8..
4173         0010: D9 32 32 D4
                                            .22.
```

```
4174          ]
4175          ]
4176        }
4177      ]},
4178    "certificate" : {
4179      "version"            : "v3",
4180      "serial number"      : "
      66F23DAF87DE8BB14AEA0C573101C2EC",
4181      "signature algorithm": "SHA384withECDSA",
4182      "issuer"             : "CN=Microsoft ECC Root
       Certificate Authority 2017, O=Microsoft
      Corporation, C=US",
4183      "not before"         : "2019-12-19 07:06:45.
      000 SGT",
4184      "not  after"         : "2042-07-19 07:16:04.
      000 SGT",
4185      "subject"            : "CN=Microsoft ECC Root
       Certificate Authority 2017, O=Microsoft
      Corporation, C=US",
4186      "subject public key" : "EC",
4187      "extensions"         : [
4188        {
4189          ObjectId: 1.3.6.1.4.1.311.21.1
      Criticality=false
4190        },
4191        {
4192          ObjectId: 2.5.29.19 Criticality=true
4193          BasicConstraints:[
4194            CA:true
4195            PathLen: no limit
4196          ]
4197        },
4198        {
4199          ObjectId: 2.5.29.15 Criticality=true
4200          KeyUsage [
4201            DigitalSignature
4202            Key_CertSign
4203            Crl_Sign
4204          ]
4205        },
4206        {
```

```
4207         ObjectId: 2.5.29.14 Criticality=false
4208         SubjectKeyIdentifier [
4209         KeyIdentifier [
4210         0000: C8 CB 99 72 70 52 0C F8   E6 BE B2
     04 57 29 2A CF  ...rpR......W)*.
4211         0010: 42 10 ED 35
                                            B..5
4212         ]
4213         ]
4214       }
4215     ]},
4216   "certificate" : {
4217     "version"            : "v3",
4218     "serial number"      : "7497258AC73F7A54",
4219     "signature algorithm": "SHA384withECDSA",
4220     "issuer"             : "CN=AffirmTrust
     Premium ECC, O=AffirmTrust, C=US",
4221     "not before"         : "2010-01-29 22:20:24.
     000 SGT",
4222     "not  after"         : "2040-12-31 22:20:24.
     000 SGT",
4223     "subject"            : "CN=AffirmTrust
     Premium ECC, O=AffirmTrust, C=US",
4224     "subject public key" : "EC",
4225     "extensions"         : [
4226       {
4227         ObjectId: 2.5.29.19 Criticality=true
4228         BasicConstraints:[
4229           CA:true
4230           PathLen: no limit
4231         ]
4232       },
4233       {
4234         ObjectId: 2.5.29.15 Criticality=true
4235         KeyUsage [
4236           Key_CertSign
4237           Crl_Sign
4238         ]
4239       },
4240       {
4241         ObjectId: 2.5.29.14 Criticality=false
```

```
4242         SubjectKeyIdentifier [
4243         KeyIdentifier [
4244         0000: 9A AF 29 7A C0 11 35 35   26 51 30
     00 C3 6A FE 40  ..)z..55&Q0..j.@
4245         0010: D5 AE D6 3C
                                                ...<
4246         ]
4247         ]
4248       }
4249     ]},
4250   "certificate" : {
4251     "version"            : "v3",
4252     "serial number"      : "01",
4253     "signature algorithm": "SHA256withRSA",
4254     "issuer"             : "CN=T-TeleSec
     GlobalRoot Class 2, OU=T-Systems Trust Center, O=
     T-Systems Enterprise Services GmbH, C=DE",
4255     "not before"         : "2008-10-01 18:40:14.
     000 SGT",
4256     "not  after"         : "2033-10-02 07:59:59.
     000 SGT",
4257     "subject"            : "CN=T-TeleSec
     GlobalRoot Class 2, OU=T-Systems Trust Center, O=
     T-Systems Enterprise Services GmbH, C=DE",
4258     "subject public key" : "RSA",
4259     "extensions"         : [
4260       {
4261         ObjectId: 2.5.29.19 Criticality=true
4262         BasicConstraints:[
4263           CA:true
4264           PathLen: no limit
4265         ]
4266       },
4267       {
4268         ObjectId: 2.5.29.15 Criticality=true
4269         KeyUsage [
4270           Key_CertSign
4271           Crl_Sign
4272         ]
4273       },
4274       {
```

```
4275         ObjectId: 2.5.29.14 Criticality=false
4276         SubjectKeyIdentifier [
4277         KeyIdentifier [
4278         0000: BF 59 20 36 00 79 A0 A0   22 6B 8C
     D5 F2 61 D2 B8  .Y 6.y.."k...a..
4279         0010: 2C CB 82 4A
                                             ,..J
4280         ]
4281         ]
4282       }
4283     ]},
4284   "certificate" : {
4285     "version"            : "v3",
4286     "serial number"      : "
     033AF1E6A711A9A0BB2864B11D09FAE5",
4287     "signature algorithm": "SHA256withRSA",
4288     "issuer"             : "CN=DigiCert Global
     Root G2, OU=www.digicert.com, O=DigiCert Inc, C=
     US",
4289     "not before"         : "2013-08-01 20:00:00.
     000 SGT",
4290     "not  after"         : "2038-01-15 20:00:00.
     000 SGT",
4291     "subject"            : "CN=DigiCert Global
     Root G2, OU=www.digicert.com, O=DigiCert Inc, C=
     US",
4292     "subject public key" : "RSA",
4293     "extensions"         : [
4294       {
4295         ObjectId: 2.5.29.19 Criticality=true
4296         BasicConstraints:[
4297           CA:true
4298           PathLen: no limit
4299         ]
4300       },
4301       {
4302         ObjectId: 2.5.29.15 Criticality=true
4303         KeyUsage [
4304           DigitalSignature
4305           Key_CertSign
4306           Crl_Sign
```

```
4307         ]
4308       },
4309       {
4310         ObjectId: 2.5.29.14 Criticality=false
4311         SubjectKeyIdentifier [
4312         KeyIdentifier [
4313         0000: 4E 22 54 20 18 95 E6 E3   6E E6 0F
     FA FA B9 12 ED  N"T ....n.......
4314         0010: 06 17 8F 39
                                                ...9
4315         ]
4316         ]
4317       }
4318     ]}
4319 )
4320 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.273 SGT|SSLContextImpl.java:
     115|trigger seeding of SecureRandom
4321 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.273 SGT|SSLContextImpl.java:
     119|done seeding of SecureRandom
4322 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.277 SGT|SSLConfiguration.java
     :461|System property jdk.tls.server.
     SignatureSchemes is set to 'null'
4323 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.284 SGT|SSLConfiguration.java
     :461|System property jdk.tls.client.
     SignatureSchemes is set to 'null'
4324 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.284 SGT|SSLContextImpl.java:
     115|trigger seeding of SecureRandom
4325 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.284 SGT|SSLContextImpl.java:
     119|done seeding of SecureRandom
4326 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.285 SGT|SSLContextImpl.java:
     115|trigger seeding of SecureRandom
4327 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.285 SGT|SSLContextImpl.java:
     119|done seeding of SecureRandom
```

```
4328 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.285 SGT|X509TrustManagerImpl.
     java:82|adding as trusted certificates (
4329   "certificate" : {
4330     "version"            : "v3",
4331     "serial number"      : "
     06ABF573EEEC3D05F2E90F1FC867045899AA7D5E",
4332     "signature algorithm": "SHA256withRSA",
4333     "issuer"             : "CN=localhost, OU=IN,
     O=IN, L=IN, ST=IN, C=IN",
4334     "not before"         : "2024-10-31 15:15:27.
     000 SGT",
4335     "not  after"         : "2025-10-31 15:15:27.
     000 SGT",
4336     "subject"            : "CN=localhost, OU=IN,
     O=IN, L=IN, ST=IN, C=IN",
4337     "subject public key" : "RSA",
4338     "extensions"         : [
4339       {
4340         ObjectId: 2.5.29.14 Criticality=false
4341         SubjectKeyIdentifier [
4342         KeyIdentifier [
4343         0000: 33 9D C9 0B 0D 9C 77 75   AC 5F 2F
     EA BB D6 76 D6  3.....wu._/...v.
4344         0010: 5A 88 3B 7F
                                            Z.;.
4345         ]
4346         ]
4347       }
4348     ]}
4349 )
4350 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.285 SGT|SSLContextImpl.java:
     115|trigger seeding of SecureRandom
4351 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.285 SGT|SSLContextImpl.java:
     119|done seeding of SecureRandom
4352 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 for TLSv1
```

```
4352 .3
4353 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 for TLSv1
     .3
4354 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 for TLSv1.3
4355 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 for TLSv1.3
4356 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA for TLSv1.3
4357 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA for TLSv1.3
4358 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_RSA_WITH_AES_128_GCM_SHA256 for TLSv1.3
4359 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_RSA_WITH_AES_128_CBC_SHA for TLSv1.3
4360 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.306 SGT|HandshakeContext.java
     :298|Ignore unsupported cipher suite:
     TLS_RSA_WITH_AES_256_CBC_SHA for TLSv1.3
4361 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.310 SGT|SSLExtension.java:824
     |System property jdk.tls.client.disableExtensions
      is set to 'null'
4362 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.310 SGT|ServerNameExtension.
     java:266|Unable to indicate server name
```

```
4363 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.311 SGT|SSLExtensions.java:
     272|Ignore, context unavailable extension:
     server_name
4364 javax.net.ssl|INFO|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.311 SGT|AlpnExtension.java:
     182|No available application protocols
4365 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.311 SGT|SSLExtensions.java:
     272|Ignore, context unavailable extension:
     application_layer_protocol_negotiation
4366 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.311 SGT|
     SessionTicketExtension.java:408|Stateless
     resumption supported
4367 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.312 SGT|SignatureScheme.java:
     412|Ignore disabled signature scheme: rsa_md5
4368 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.312 SGT|SSLExtensions.java:
     272|Ignore, context unavailable extension: cookie
4369 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.320 SGT|PreSharedKeyExtension
     .java:661|No session to resume.
4370 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.320 SGT|SSLExtensions.java:
     272|Ignore, context unavailable extension:
     pre_shared_key
4371 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.322 SGT|ClientHello.java:641|
     Produced ClientHello handshake message (
4372 "ClientHello": {
4373   "client version"      : "TLSv1.2",
4374   "random"              : "
     342E48308B9A8EBB66E8B61D24C6AE02F7B96C72DF8ED5867
     328F9EEDF2BD7A3",
4375   "session id"          : "
     397258001E4771B0E93028E1922178F0792D80A62292EBB1C
     0888D6B2C8A4CB8",
4376   "cipher suites"       : "[
     TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(0xC02C),
```

```
4376 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(0xC02B),
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(0xC02F),
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xC030),
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xC013),
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xC014),
     TLS_RSA_WITH_AES_128_GCM_SHA256(0x009C),
     TLS_RSA_WITH_AES_128_CBC_SHA(0x002F),
     TLS_RSA_WITH_AES_256_CBC_SHA(0x0035),
     TLS_AES_128_GCM_SHA256(0x1301),
     TLS_AES_256_GCM_SHA384(0x1302)]",
4377   "compression methods" : "00",
4378   "extensions"          : [
4379     "status_request (5)": {
4380       "certificate status type": ocsp
4381       "OCSP status request": {
4382         "responder_id": <empty>
4383         "request extensions": {
4384           <empty>
4385         }
4386       }
4387     },
4388     "supported_groups (10)": {
4389       "versions": [x25519, secp256r1, secp384r1,
     secp521r1, x448, ffdhe2048, ffdhe3072, ffdhe4096
     , ffdhe6144, ffdhe8192]
4390     },
4391     "ec_point_formats (11)": {
4392       "formats": [uncompressed]
4393     },
4394     "status_request_v2 (17)": {
4395       "cert status request": {
4396         "certificate status type": ocsp_multi
4397         "OCSP status request": {
4398           "responder_id": <empty>
4399           "request extensions": {
4400             <empty>
4401           }
4402         }
4403       }
4404     },
4405     "extended_master_secret (23)": {
```

```
4406        <empty>
4407      },
4408      "session_ticket (35)": {
4409        <empty>
4410      },
4411      "signature_algorithms (13)": {
4412        "signature schemes": [
      ecdsa_secp256r1_sha256, ecdsa_secp384r1_sha384,
      ecdsa_secp521r1_sha512, ed25519, ed448,
      rsa_pss_rsae_sha256, rsa_pss_rsae_sha384,
      rsa_pss_rsae_sha512, rsa_pss_pss_sha256,
      rsa_pss_pss_sha384, rsa_pss_pss_sha512,
      rsa_pkcs1_sha256, rsa_pkcs1_sha384,
      rsa_pkcs1_sha512, dsa_sha256, ecdsa_sha224,
      rsa_sha224, dsa_sha224, ecdsa_sha1,
      rsa_pkcs1_sha1, dsa_sha1]
4413      },
4414      "supported_versions (43)": {
4415        "versions": [TLSv1.3, TLSv1.2]
4416      },
4417      "psk_key_exchange_modes (45)": {
4418        "ke_modes": [psk_dhe_ke]
4419      },
4420      "signature_algorithms_cert (50)": {
4421        "signature schemes": [
      ecdsa_secp256r1_sha256, ecdsa_secp384r1_sha384,
      ecdsa_secp521r1_sha512, ed25519, ed448,
      rsa_pss_rsae_sha256, rsa_pss_rsae_sha384,
      rsa_pss_rsae_sha512, rsa_pss_pss_sha256,
      rsa_pss_pss_sha384, rsa_pss_pss_sha512,
      rsa_pkcs1_sha256, rsa_pkcs1_sha384,
      rsa_pkcs1_sha512, dsa_sha256, ecdsa_sha224,
      rsa_sha224, dsa_sha224, ecdsa_sha1,
      rsa_pkcs1_sha1, dsa_sha1]
4422      },
4423      "key_share (51)": {
4424        "client_shares": [
4425          {
4426            "named group": x25519
4427            "key_exchange": {
4428              0000: 15 8B 72 AE 88 5D E2 88   03 50
```

```
4428  02 E4 85 B4 98 1F  ..r..]...P......
4429             0010: 65 80 0C F4 62 86 A1 0B   A7 7D
      2B 1F 8E 3D F7 5F  e...b.....+..=._
4430           }
4431         },
4432         {
4433           "named group": secp256r1
4434           "key_exchange": {
4435             0000: 04 1A 15 C3 9C 55 93 BF   F1 D6
      3F 01 0F DA 24 4B  .....U....?...$K
4436             0010: 23 37 59 B6 17 18 D2 95   EB 5B
      73 CC 03 62 28 05  #7Y......[s..b(.
4437             0020: 22 B1 65 C5 77 A8 AC EA   35 25
      3A 6B 75 AE 41 AD  ".e.w...5%:ku.A.
4438             0030: 77 19 5B 70 E0 63 0E 76   00 0A
      23 90 9A 17 A0 6F  w.[p.c.v..#....o
4439             0040: 65
4440           }
4441         },
4442       ]
4443     },
4444     "renegotiation_info (65,281)": {
4445       "renegotiated connection": [<no
     renegotiated connection>]
4446     }
4447   ]
4448 }
4449 )
4450 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.323 SGT|SSLEngineOutputRecord
     .java:530|WRITE: TLSv1.3 handshake, length = 388
4451 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.323 SGT|SSLEngineOutputRecord
     .java:551|Raw write (
4452   0000: 16 03 03 01 84 01 00 01   80 03 03 34 2E
     48 30 8B  ...........4.H0.
4453   0010: 9A 8E BB 66 E8 B6 1D 24   C6 AE 02 F7 B9
     6C 72 DF  ...f...$.....lr.
4454   0020: 8E D5 86 73 28 F9 EE DF   2B D7 A3 20 39
     72 58 00  ...s(...+.. 9rX.
4455   0030: 1E 47 71 B0 E9 30 28 E1   92 21 78 F0 79
```

```
4455 2D 80 A6  .Gq..0(..!x.y-..
4456   0040: 22 92 EB B1 C0 88 8D 6B   2C 8A 4C B8 00
     16 C0 2C  "......k,.L....,
4457   0050: C0 2B C0 2F C0 30 C0 13   C0 14 00 9C 00
     2F 00 35  .+./.0......./.5
4458   0060: 13 01 13 02 01 00 01 21   00 05 00 05 01
     00 00 00  .......!........
4459   0070: 00 00 0A 00 16 00 14 00   1D 00 17 00 18
     00 19 00  ................
4460   0080: 1E 01 00 01 01 01 02 01   03 01 04 00 0B
     00 02 01  ................
4461   0090: 00 00 11 00 09 00 07 02   00 04 00 00 00
     00 00 17  ................
4462   00A0: 00 00 00 23 00 00 00 0D   00 2C 00 2A 04
     03 05 03  ...#.....,.*....
4463   00B0: 06 03 08 07 08 08 08 04   08 05 08 06 08
     09 08 0A  ................
4464   00C0: 08 0B 04 01 05 01 06 01   04 02 03 03 03
     01 03 02  ................
4465   00D0: 02 03 02 01 02 02 00 2B   00 05 04 03 04
     03 03 00  .......+........
4466   00E0: 2D 00 02 01 01 00 32 00   2C 00 2A 04 03
     05 03 06  -.....2.,.*.....
4467   00F0: 03 08 07 08 08 08 04 08   05 08 06 08 09
     08 0A 08  ................
4468   0100: 0B 04 01 05 01 06 01 04   02 03 03 03 01
     03 02 02  ................
4469   0110: 03 02 01 02 02 00 33 00   6B 00 69 00 1D
     00 20 15  ......3.k.i... .
4470   0120: 8B 72 AE 88 5D E2 88 03   50 02 E4 85 B4
     98 1F 65  .r..]...P......e
4471   0130: 80 0C F4 62 86 A1 0B A7   7D 2B 1F 8E 3D
     F7 5F 00  ...b.....+..=._.
4472   0140: 17 00 41 04 1A 15 C3 9C   55 93 BF F1 D6
     3F 01 0F  ..A.....U....?..
4473   0150: DA 24 4B 23 37 59 B6 17   18 D2 95 EB 5B
     73 CC 03  .$K#7Y......[s..
4474   0160: 62 28 05 22 B1 65 C5 77   A8 AC EA 35 25
     3A 6B 75  b(."e.w...5%:ku
4475   0170: AE 41 AD 77 19 5B 70 E0   63 0E 76 00 0A
     23 90 9A  .A.w.[p.c.v..#..
```

```
4476   0180: 17 A0 6F 65 FF 01 00 01   00
                           ..oe.....
4477 )
4478 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.330 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4479   0000: 16 03 03 00 7A 02 00 00   76 03 03 D9 62
     16 BE 2E  ....z...v...b...
4480   0010: CD DD 8D F8 17 0E DB BA   10 0B 80 34 27
     A4 50 47  ...........4'.PG
4481   0020: 8E 86 92 BD EC C8 38 8A   D6 30 B2 20 39
     72 58 00  ......8..0. 9rX.
4482   0030: 1E 47 71 B0 E9 30 28 E1   92 21 78 F0 79
     2D 80 A6  .Gq..0(..!x.y-..
4483   0040: 22 92 EB B1 C0 88 8D 6B   2C 8A 4C B8 13
     01 00 00  ".....k,.L.....
4484   0050: 2E 00 2B 00 02 03 04 00   33 00 24 00 1D
     00 20 41  ..+.....3.$... A
4485   0060: 68 66 D1 63 6D 1A B8 5F   88 D0 86 13 F6
     54 CB AD  hf.cm.._.....T..
4486   0070: BF 71 3B CC 7F 0F D3 90   57 3B 45 2C 43
     7B 7F     .q;.....W;E,C..
4487 )
4488 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.330 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 handshake, length = 122
4489 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|ServerHello.java:888|
     Consuming ServerHello handshake message (
4490 "ServerHello": {
4491   "server version"      : "TLSv1.2",
4492   "random"              : "
     D96216BE2ECDDD8DF8170EDBBA100B803427A450478E8692B
     DECC8388AD630B2",
4493   "session id"          : "
     397258001E4771B0E93028E1922178F0792D80A62292EBB1C
     0888D6B2C8A4CB8",
4494   "cipher suite"        : "TLS_AES_128_GCM_SHA256
     (0x1301)",
4495   "compression methods" : "00",
4496   "extensions"          : [
```

```
4497     "supported_versions (43)": {
4498       "selected version": [TLSv1.3]
4499     },
4500     "key_share (51)": {
4501       "server_share": {
4502         "named group": x25519
4503         "key_exchange": {
4504           0000: 41 68 66 D1 63 6D 1A B8   5F 88
     D0 86 13 F6 54 CB  Ahf.cm.._.....T.
4505           0010: AD BF 71 3B CC 7F 0F D3   90 57
     3B 45 2C 43 7B 7F  ..q;.....W;E,C..
4506         }
4507       },
4508     }
4509   ]
4510 }
4511 )
4512 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     204|Consumed extension: supported_versions
4513 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|ServerHello.java:984|
     Negotiated protocol version: TLSv1.3
4514 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension: server_name
4515 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension:
     max_fragment_length
4516 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension: status_request
4517 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension:
     ec_point_formats
4518 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension:
     application_layer_protocol_negotiation
```

```
4519 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension:
     status_request_v2
4520 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension:
     extended_master_secret
4521 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     175|Ignore unsupported extension: session_ticket
4522 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.331 SGT|SSLExtensions.java:
     204|Consumed extension: supported_versions
4523 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     204|Consumed extension: key_share
4524 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     175|Ignore unsupported extension:
     renegotiation_info
4525 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|PreSharedKeyExtension
     .java:924|Handling pre_shared_key absence.
4526 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLSessionImpl.java:
     219|Session initialized:  Session(1730444763332|
     TLS_AES_128_GCM_SHA256)
4527 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension: server_name
4528 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     max_fragment_length
4529 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension: status_request
4530 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
```

```
4530 ec_point_formats
4531 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     application_layer_protocol_negotiation
4532 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     status_request_v2
4533 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     extended_master_secret
4534 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension: session_ticket
4535 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     227|Ignore impact of unsupported extension:
     supported_versions
4536 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     227|Ignore impact of unsupported extension:
     key_share
4537 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     renegotiation_info
4538 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.332 SGT|SSLExtensions.java:
     219|Ignore unavailable extension: pre_shared_key
4539 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.335 SGT|SSLCipher.java:1870|
     KeyLimit read side: algorithm = AES/GCM/NOPADDING
     :KEYUPDATE
4540 countdown value = 137438953472
4541 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.335 SGT|SSLCipher.java:2024|
     KeyLimit write side: algorithm = AES/GCM/
     NOPADDING:KEYUPDATE
4542 countdown value = 137438953472
```

```
4543 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.335 SGT|SSLEngineOutputRecord
     .java:530|WRITE: TLSv1.3 change_cipher_spec,
     length = 1
4544 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.335 SGT|SSLEngineOutputRecord
     .java:551|Raw write (
4545   0000: 14 03 03 00 01 01
                                          ......
4546 )
4547 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.336 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4548   0000: 14 03 03 00 01 01
                                          ......
4549 )
4550 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.336 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 change_cipher_spec, length
      = 1
4551 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.336 SGT|ChangeCipherSpec.java
     :246|Consuming ChangeCipherSpec message
4552 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.336 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4553   0000: 17 03 03 00 17 61 BE 6A   E3 B4 6B B4 2F
     16 4B 6E  .....a.j..k./.Kn
4554   0010: 80 F5 70 94 C2 5F 70 5C   CB CC 5F E8
                  ..p.._p\.._.
4555 )
4556 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.336 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 23
4557 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
4558   0000: 08 00 00 02 00 00
                                          ......
4559 )
```

```
4560 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|EncryptedExtensions.
     java:171|Consuming EncryptedExtensions handshake
     message (
4561 "EncryptedExtensions": [
4562   <no extension>
4563 ]
4564 )
4565 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLExtensions.java:
     185|Ignore unavailable extension: server_name
4566 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLExtensions.java:
     185|Ignore unavailable extension:
     max_fragment_length
4567 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLExtensions.java:
     185|Ignore unavailable extension:
     supported_groups
4568 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLExtensions.java:
     219|Ignore unavailable extension: server_name
4569 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     max_fragment_length
4570 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     supported_groups
4571 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     application_layer_protocol_negotiation
4572 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4573   0000: 17 03 03 00 44 53 71 9B   65 FE 25 56 3B
     A1 DA 11  ....DSq.e.%V;...
4574   0010: E5 1C FB C7 6A 9B 35 B9   14 B1 42 B9 0B
     36 8C B1  ....j.5...B..6..
```

```
4575   0020: 36 0B 0A B9 65 5A 8A 84   7B C0 DB 64 0A
     DF 80 4C  6...eZ.....d...L
4576   0030: 51 B0 BD 31 22 E9 E5 66   46 E0 79 B0 15
     96 D1 2D  Q..1"..fF.y....-
4577   0040: 20 FB 05 BC A0 19 AE F8   9B
                              ........
4578 )
4579 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 68
4580 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.337 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
4581   0000: 0D 00 00 2F 00 00 2C 00   0D 00 28 00 26
     04 03 05  .../..,...(.&...
4582   0010: 03 06 03 08 07 08 08 08   1A 08 1B 08 1C
     08 09 08  ................
4583   0020: 0A 08 0B 08 04 08 05 08   06 04 01 05 01
     06 01 03  ................
4584   0030: 03 03 01
                                                  ...
4585 )
4586 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|CertificateRequest.
     java:978|Consuming CertificateRequest handshake
     message (
4587 "CertificateRequest": {
4588   "certificate_request_context": "",
4589   "extensions": [
4590     "signature_algorithms (13)": {
4591       "signature schemes": [
     ecdsa_secp256r1_sha256, ecdsa_secp384r1_sha384,
     ecdsa_secp521r1_sha512, ed25519, ed448, UNDEFINED
     -SIGNATURE(26)_UNDEFINED-HASH(8), UNDEFINED-
     SIGNATURE(27)_UNDEFINED-HASH(8), UNDEFINED-
     SIGNATURE(28)_UNDEFINED-HASH(8),
     rsa_pss_pss_sha256, rsa_pss_pss_sha384,
     rsa_pss_pss_sha512, rsa_pss_rsae_sha256,
     rsa_pss_rsae_sha384, rsa_pss_rsae_sha512,
     rsa_pkcs1_sha256, rsa_pkcs1_sha384,
```

```
4591 rsa_pkcs1_sha512, ecdsa_sha224, rsa_sha224]
4592     }
4593   ]
4594 }
4595 )
4596 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLExtensions.java:
     204|Consumed extension: signature_algorithms
4597 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLExtensions.java:
     185|Ignore unavailable extension:
     certificate_authorities
4598 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLExtensions.java:
     185|Ignore unavailable extension:
     signature_algorithms_cert
4599 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.338 SGT|SignatureScheme.java
     :434|Unsupported signature scheme: UNDEFINED-
     SIGNATURE(26)_UNDEFINED-HASH(8)
4600 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.338 SGT|SignatureScheme.java
     :434|Unsupported signature scheme: UNDEFINED-
     SIGNATURE(27)_UNDEFINED-HASH(8)
4601 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.338 SGT|SignatureScheme.java
     :434|Unsupported signature scheme: UNDEFINED-
     SIGNATURE(28)_UNDEFINED-HASH(8)
4602 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.338 SGT|SignatureScheme.java
     :446|Unsupported signature scheme: ecdsa_sha224
4603 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.338 SGT|SignatureScheme.java
     :446|Unsupported signature scheme: rsa_sha224
4604 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLExtensions.java:
     236|Populated with extension:
     signature_algorithms
4605 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
```

```
4605 certificate_authorities
4606 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLExtensions.java:
     219|Ignore unavailable extension:
     signature_algorithms_cert
4607 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4608   0000: 17 03 03 03 7B 80 4D 2A   05 C8 DF DA 71
     38 87 85  ......M*....q8..
4609   0010: 4E 65 C9 FB 33 7D DE 43   23 D4 5F 42 20
     07 5E 98  Ne..3..C#._B .^.
4610   0020: 03 3C 5E ED 47 84 85 BB   D3 FD B9 78 E0
     F4 CB E9  .<^.G......x....
4611   0030: 08 60 EE DF C1 5E 87 4A   9B 8C 4A BB 88
     7E D5 32  .`...^.J..J....2
4612   0040: 55 DF 91 9E EF F4 E8 14   76 09 4A CD BB
     D6 0C 4D  U.......v.J....M
4613   0050: 94 00 22 40 49 59 E0 84   73 A1 C2 E9 35
     D5 AC 1E  .."@IY..s...5...
4614   0060: 3E 00 42 4C 2E 51 A6 49   DF C9 1C 08 CF
     46 D2 13  >.BL.Q.I.....F..
4615   0070: 5D 0B 9C 44 9C 7A 62 85   0A 70 64 C2 AF
     A1 98 C8  ]..D.zb..pd.....
4616   0080: 20 FA 74 A1 36 7B DF 0F   B1 7A 63 75 C0
     68 4F 82   .t.6....zcu.hO.
4617   0090: 09 48 D7 75 82 2D F9 05   C6 A5 7B AA 56
     99 A7 CF  .H.u.-......V...
4618   00A0: B0 6F E6 59 EE 8F 2D 73   D0 40 58 76 F0
     5E C8 7F  .o.Y..-s.@Xv.^..
4619   00B0: 38 EE 60 E3 BC 03 4A 2D   2F 9A DD 78 7B
     39 8E B0  8.`...J-/..x.9..
4620   00C0: 80 DC E9 A3 75 43 20 F0   62 F0 5C AC 48
     64 5B 71  ....uC .b.\.Hd[q
4621   00D0: 6C D1 CE E0 1E C0 DF 83   46 69 60 4E 14
     7C F0 1D  l.......Fi`N....
4622   00E0: B4 E5 A3 02 57 DE 0E CA   22 CD 4A 18 7F
     2E 01 7B  ....W..."".J.....
4623   00F0: A1 BB 1A BE F5 EB BD FC   1E 41 21 23 FE
     AF 19 16  .........A!#....
4624   0100: AC 03 C3 2B 78 C1 A2 B0   4A 0A 19 C8 49
```

```
4624 90 DF 9C  ...+x...J...I...
4625   0110: 68 16 3D 80 C8 10 E4 46   B1 EB 2C B0 44
     11 25 97  h.=....F..,.D.%.
4626   0120: 12 3D ED 7C 28 E9 CA E0   AA 81 6D E6 E9
     5C AC 95  .=..(.....m..\..
4627   0130: C5 9D 5B 68 D6 D1 90 02   9C 23 62 90 61
     6A 68 B0  ..[h.....#b.ajh.
4628   0140: A7 85 00 CB 54 6A 21 15   28 6A 15 91 68
     E3 CD 43  ....Tj!.(j..h..C
4629   0150: 56 39 B9 A0 C7 48 93 DB   2F 7C F0 ED B6
     B2 47 A0  V9...H../.....G.
4630   0160: D7 64 78 62 2B 8F 0A FA   F8 C2 D9 68 ED
     1F BD 27  .dxb+......h...'
4631   0170: E6 D0 0F E2 C8 3F 14 DE   7F 9E 64 45 8E
     88 CE C5  .....?....dE....
4632   0180: 6F F5 F1 65 28 2B E1 15   5E 02 1A 39 65
     5F A0 F3  o..e(+..^..9e_..
4633   0190: 99 41 33 69 98 BE E2 FD   87 6F 09 3A 34
     DF 0E BE  .A3i.....o.:4...
4634   01A0: 47 04 E9 72 05 5B CB 99   B4 20 F0 06 39
     AE 02 14  G..r.[... ..9...
4635   01B0: D9 07 93 7E 7F 85 F0 28   A3 0F 6A D8 0B
     6B 17 47  .......(..j..k.G
4636   01C0: B3 38 EF D6 BB 88 B5 C3   01 F5 F3 C1 9E
     23 58 93  .8..........#X.
4637   01D0: FA 03 E4 63 8A A9 01 10   FB 06 EA FF 4F
     97 E9 75  ...c........O..u
4638   01E0: 83 69 8A 8F 24 24 F8 C7   AA 43 32 73 30
     81 EE C5  .i..$$...C2s0...
4639   01F0: 78 C6 EC BF 97 19 1A 64   1C 69 9A 83 71
     1D 1C 50  x......d.i..q..P
4640   0200: 94 29 FD 9C EF A4 9E 77   5F 7F C3 06 13
     74 FD 08  .).....w_....t..
4641   0210: 1B 5F C0 51 0C B2 F6 02   93 C2 FE EA C8
     88 A2 C9  ._.Q.............
4642   0220: 27 95 F3 8F 12 DC 57 51   E3 8B F1 C8 A9
     E5 65 43  '.....WQ......eC
4643   0230: 78 38 13 8F AA 7D 2A F3   E7 BB 1D 63 CA
     61 AB 6F  x8....*....c.a.o
4644   0240: D4 BF 3E 6F CB A1 6F E9   02 D4 62 6F 1A
     AF A4 8F  ..>o..o...bo....
```

```
4645   0250: 98 D7 92 B4 9F 7C 1A FB   8B 00 9F B1 05
     45 B5 0F  .............E..
4646   0260: 59 56 BF 58 69 92 75 34   DF AB 18 57 AE
     47 5C 09  YV.Xi.u4...W.G\.
4647   0270: 2D 9D FD A9 FF 6E B9 A9   FE 6A 94 D6 15
     54 CE 5E  -....n...j...T.^
4648   0280: 41 7D 4B 9B 61 46 91 1E   D1 F7 A0 C9 46
     0F C6 75  A.K.aF......F..u
4649   0290: 14 F6 30 AC D4 00 5D A9   46 81 00 03 E4
     2F 60 CE  ..0...].F..../`.
4650   02A0: 2C B7 34 2C 61 70 13 46   3D FA CD 16 2F
     0C 54 B2  ,.4,ap.F=.../.T.
4651   02B0: 25 D7 A8 B8 A6 17 C5 6C   87 BF 08 40 6E
     31 8E C7  %......l...@n1..
4652   02C0: BE C4 23 86 37 35 53 96   CA 20 EF 9A 39
     86 F0 C8  ..#.75S.. ..9...
4653   02D0: 31 E2 91 40 BE 9D 9F 3A   3B 43 D0 BA DB
     72 B2 3F  1..@...:;C...r.?
4654   02E0: BC 35 F5 92 C9 49 DD 91   2F 15 9B 52 0D
     B8 47 A7  .5...I../..R..G.
4655   02F0: DE 7B B3 C1 22 BD 4C E6   C7 26 17 FD F9
     41 6F 8C  ....".L..&...Ao.
4656   0300: 81 26 FD 6C BB 76 94 5B   5F 03 D0 A2 89
     10 53 0A  .&.l.v.[_.....S.
4657   0310: 7E 3B 34 7D 60 FB 44 FD   B9 60 CE 22 A5
     CE 56 07  .;4.`.D..`."..V.
4658   0320: 29 44 1C 66 9E 9B 05 0F   86 DB 60 45 73
     3C AF 58  )D.f......`Es<.X
4659   0330: 4A 09 AD 06 9A BA CA 80   19 82 CC A0 2D
     D1 BB 70  J...........-..p
4660   0340: 0B 4B E8 32 AD A4 42 5C   90 D8 29 6F 62
     76 C1 47  .K.2..B\..)obv.G
4661   0350: 6B DC D1 F4 91 EF 0C 42   F6 EF 0D 23 C5
     6B CD 42  k......B...#.k.B
4662   0360: 86 D1 50 68 40 11 29 F5   C7 FE BC 94 FF
     39 14 06  ..Ph@.)......9..
4663   0370: BC E9 BD CD 7E CE EC 6B   9A 6B A8 EF DE
     BF 3A 9C  .......k.k....:.
4664 )
4665 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.338 SGT|SSLEngineInputRecord.
```

```
4665 java:213|READ: TLSv1.2 application_data, length
      = 891
4666 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.339 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
4667   0000: 0B 00 03 66 00 00 03 62   00 03 5D 30 82
     03 59 30  ...f...b..]0..Y0
4668   0010: 82 02 41 A0 03 02 01 02   02 14 06 AB F5
     73 EE EC  ..A.........s..
4669   0020: 3D 05 F2 E9 0F 1F C8 67   04 58 99 AA 7D
     5E 30 0D  =......g.X...^0.
4670   0030: 06 09 2A 86 48 86 F7 0D   01 01 0B 05 00
     30 55 31  ..*.H........0U1
4671   0040: 0B 30 09 06 03 55 04 06   13 02 49 4E 31
     0B 30 09  .0...U....IN1.0.
4672   0050: 06 03 55 04 08 0C 02 49   4E 31 0B 30 09
     06 03 55  ..U....IN1.0...U
4673   0060: 04 07 0C 02 49 4E 31 0B   30 09 06 03 55
     04 0A 0C  ....IN1.0...U...
4674   0070: 02 49 4E 31 0B 30 09 06   03 55 04 0B 0C
     02 49 4E  .IN1.0...U....IN
4675   0080: 31 12 30 10 06 03 55 04   03 0C 09 6C 6F
     63 61 6C  1.0...U....local
4676   0090: 68 6F 73 74 30 1E 17 0D   32 34 31 30 33
     31 30 37  host0...24103107
4677   00A0: 31 35 32 37 5A 17 0D 32   35 31 30 33 31
     30 37 31  1527Z..251031071
4678   00B0: 35 32 37 5A 30 55 31 0B   30 09 06 03 55
     04 06 13  527Z0U1.0...U...
4679   00C0: 02 49 4E 31 0B 30 09 06   03 55 04 08 0C
     02 49 4E  .IN1.0...U....IN
4680   00D0: 31 0B 30 09 06 03 55 04   07 0C 02 49 4E
     31 0B 30  1.0...U....IN1.0
4681   00E0: 09 06 03 55 04 0A 0C 02   49 4E 31 0B 30
     09 06 03  ...U....IN1.0...
4682   00F0: 55 04 0B 0C 02 49 4E 31   12 30 10 06 03
     55 04 03  U....IN1.0...U..
4683   0100: 0C 09 6C 6F 63 61 6C 68   6F 73 74 30 82
     01 22 30  ..localhost0.."0
4684   0110: 0D 06 09 2A 86 48 86 F7   0D 01 01 01 05
     00 03 82  ...*.H.........
```

```
4685   0120: 01 0F 00 30 82 01 0A 02   82 01 01 00 CA
     B5 2D E1  ...0.........-.
4686   0130: 0C BA B1 DF 5D 09 32 B2   70 72 E7 84 9B
     C6 91 C3  ....].2.pr.....
4687   0140: 4A 3B 98 86 64 BE 75 F6   3D 3E 46 A0 24
     2E 77 EB  J;..d.u.=>F.$.w.
4688   0150: A0 8D 23 F9 6E E7 7B 2D   C7 34 2D 79 8F
     E9 05 64  ..#.n..-.4-y...d
4689   0160: FE 59 94 C2 75 DC 50 3A   66 46 CB 9F 0E
     CC E9 DD  .Y..u.P:fF.....
4690   0170: A5 CF A5 45 FE E0 AE 68   79 08 5F BC FE
     A0 58 AE  ...E...hy._...X.
4691   0180: 7F 6D FE FF 76 23 74 98   03 CC 78 0D E2
     18 97 31  .m..v#t...x....1
4692   0190: A2 36 1B 43 7D CA 6D CB   C5 6A 12 8E D5
     E9 B5 68  .6.C..m..j.....h
4693   01A0: 2E 8C 93 77 8E 84 88 9F   F2 87 A0 C9 F2
     38 09 B9  ...w.........8..
4694   01B0: 95 39 31 15 35 81 14 FA   FA 06 8E D5 AB
     71 41 C2  .91.5........qA.
4695   01C0: E7 C8 F7 16 EF 4B 07 75   7E 02 00 41 59
     B8 D4 33  .....K.u...AY..3
4696   01D0: E5 AF A2 AA A6 CF B2 65   4A 38 8E B4 A1
     51 7F DC  .......eJ8...Q..
4697   01E0: B1 45 36 FD EB 3F F7 97   5E 96 F7 87 AA
     6A F9 AF  .E6..?..^....j..
4698   01F0: 8C 40 E4 72 62 DE 2B E1   A6 54 A5 20 23
     5C 82 CE  .@.rb.+..T. #\..
4699   0200: 42 A9 48 A0 49 A9 C5 67   34 3D D6 8F C3
     D3 4D F1  B.H.I..g4=....M.
4700   0210: 08 18 21 87 BF DF 1B EB   72 53 4D 77 AB
     45 1C DD  ..!.....rSMw.E..
4701   0220: 48 B0 0D BA 9F C1 33 12   81 B6 56 15 02
     03 01 00  H.....3...V.....
4702   0230: 01 A3 21 30 1F 30 1D 06   03 55 1D 0E 04
     16 04 14  ..!0.0...U......
4703   0240: 33 9D C9 0B 0D 9C 77 75   AC 5F 2F EA BB
     D6 76 D6  3.....wu._/...v.
4704   0250: 5A 88 3B 7F 30 0D 06 09   2A 86 48 86 F7
     0D 01 01  Z.;.0...*.H.....
4705   0260: 0B 05 00 03 82 01 01 00   63 8F F0 32 E3
```

```
4705 4F AD 36  ........c..2.O.6
4706   0270: 2F 6A C7 CE 2E A5 BF 7B   C6 AA 83 31 D5
     4E DD 67  /j.........1.N.g
4707   0280: E4 33 63 21 02 F0 A8 11   31 C5 38 FC 1B
     2C 61 C7  .3c!....1.8..,a.
4708   0290: 95 93 8A 09 AD CA 4D 05   01 79 87 8A 3E
     18 12 A3  ......M..y..>...
4709   02A0: 2F 4E 85 36 12 13 92 9C   13 0A AF 42 D2
     63 3D EB  /N.6.......B.c=.
4710   02B0: 92 CD 59 8C AF D9 37 2C   F3 A3 3E AE 7E
     0C 74 40  ..Y...7,..>...t@
4711   02C0: 58 76 A3 CE 9D 79 45 70   AF 2B C5 5E BD
     65 03 70  Xv...yEp.+.^.e.p
4712   02D0: 8D CC A4 CB EE E0 DF 53   D2 3B D7 1B 93
     85 89 48  .......S.;.....H
4713   02E0: 8A 61 5D FE 1F E2 83 CE   38 D9 2C 24 90
     33 F9 12  .a].....8.,$.3..
4714   02F0: B0 D9 AA FE 26 C2 81 62   83 61 94 F9 FC
     D1 CA 22  ....&..b.a....."
4715   0300: C5 24 AD BC B8 73 27 49   DF 9C 58 C0 65
     A5 52 C1  .$...s'I..X.e.R.
4716   0310: 42 44 94 71 3C C3 6F 5C   76 8B AB 81 0F
     8A 2E A8  BD.q<.o\v.......
4717   0320: F5 3F 3D E3 49 E2 9E 11   E8 1B 01 2E 34
     53 2F 29  .?=.I.......4S/)
4718   0330: B8 71 9E B6 9F 7D 6C F0   E6 95 FA 8A F4
     B3 0D EF  .q....l.........
4719   0340: A4 70 8A FF 3B 39 DF A9   39 19 29 C8 48
     0E 54 0B  .p..;9..9.).H.T.
4720   0350: DE 5A 3C 05 4A 68 3E 7F   2E 53 CC 52 78
     83 FB 52  .Z<.Jh>..S.Rx..R
4721   0360: 66 B1 B1 D6 1B A8 D0 79   00 00
                        f......y..
4722 )
4723 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.340 SGT|CertificateMessage.
     java:1166|Consuming server Certificate handshake
     message (
4724 "Certificate": {
4725   "certificate_request_context": "",
4726   "certificate_list": [
```

```
4727   {
4728     "certificate" : {
4729       "version"            : "v3",
4730       "serial number"      : "
     06ABF573EEEC3D05F2E90F1FC867045899AA7D5E",
4731       "signature algorithm": "SHA256withRSA",
4732       "issuer"             : "CN=localhost, OU=IN
     , O=IN, L=IN, ST=IN, C=IN",
4733       "not before"         : "2024-10-31 15:15:27
     .000 SGT",
4734       "not  after"         : "2025-10-31 15:15:27
     .000 SGT",
4735       "subject"            : "CN=localhost, OU=IN
     , O=IN, L=IN, ST=IN, C=IN",
4736       "subject public key" : "RSA",
4737       "extensions"         : [
4738         {
4739           ObjectId: 2.5.29.14 Criticality=false
4740           SubjectKeyIdentifier [
4741           KeyIdentifier [
4742           0000: 33 9D C9 0B 0D 9C 77 75   AC 5F
     2F EA BB D6 76 D6  3.....wu._/...v.
4743           0010: 5A 88 3B 7F
                                              Z.;.
4744           ]
4745           ]
4746         }
4747       ]}
4748     "extensions": {
4749       <no extension>
4750     }
4751   },
4752 ]
4753 }
4754 )
4755 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.340 SGT|SSLExtensions.java:
     185|Ignore unavailable extension: status_request
4756 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.353 SGT|X509TrustManagerImpl.
     java:301|Found trusted certificate (
```

```
4757   "certificate" : {
4758     "version"            : "v3",
4759     "serial number"      : "
     06ABF573EEEC3D05F2E90F1FC867045899AA7D5E",
4760     "signature algorithm": "SHA256withRSA",
4761     "issuer"             : "CN=localhost, OU=IN,
     O=IN, L=IN, ST=IN, C=IN",
4762     "not before"         : "2024-10-31 15:15:27.
     000 SGT",
4763     "not  after"         : "2025-10-31 15:15:27.
     000 SGT",
4764     "subject"            : "CN=localhost, OU=IN,
     O=IN, L=IN, ST=IN, C=IN",
4765     "subject public key" : "RSA",
4766     "extensions"         : [
4767       {
4768         ObjectId: 2.5.29.14 Criticality=false
4769         SubjectKeyIdentifier [
4770         KeyIdentifier [
4771         0000: 33 9D C9 0B 0D 9C 77 75   AC 5F 2F
     EA BB D6 76 D6  3.....wu._/...v.
4772         0010: 5A 88 3B 7F
                                            Z.;.
4773         ]
4774         ]
4775       }
4776     ]}
4777 )
4778 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.354 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4779   0000: 17 03 03 01 19 E1 D9 19   0D B4 F1 B0 65
     EF 18 39  ............e..9
4780   0010: 59 44 D3 7D 28 6B 5C 6E   C2 DF 96 8A C9
     8B 0A A9  YD..(k\n........
4781   0020: 3F 0F 44 C2 84 04 24 04   3D D5 3A 6D 74
     0D 31 3C  ?.D...$.=.:mt.1<
4782   0030: 04 EB 25 6A A5 CE 7C 98   C7 64 3A 3C 90
     C4 32 2F  ..%j.....d:<..2/
4783   0040: E1 6D 99 39 B7 F5 5C 24   63 6B E0 C7 40
     51 02 2C  .m.9..\$ck..@Q.,
```

```
4784   0050: C0 BA 8A BF 89 95 94 72   5B 06 F2 19 74
     BB 59 7A  .......r[...t.Yz
4785   0060: 94 C3 E8 3B 60 0C 39 A7   9C EE D8 5C 38
     97 24 34  ...;`.9....\8.$4
4786   0070: 4E 27 7E D1 BA C5 1C F5   27 0C 88 FC AA
     FB 09 E6  N'~.....'.......
4787   0080: EC 7F F6 20 CE 9A 86 3D   E9 49 17 0A 5C
     87 FA 53  ... ...=.I..\..S
4788   0090: 70 49 0C 3B 1D EA 74 C6   CB 17 FC 6A AE
     4A 17 BE  pI.;..t....j.J..
4789   00A0: 67 86 58 80 9A 60 D1 1F   9B 2C 2C 48 CE
     E1 7A B5  g.X..`...,,H..z.
4790   00B0: 70 27 48 0D D8 1A 2E F7   06 E7 D0 7A B3
     A4 60 DA  p'H........z..`.
4791   00C0: AC 76 2E 33 0D BE 75 02   22 19 5F 90 D7
     91 CA 15  .v.3..u."._.....
4792   00D0: FA BE 4F F6 6E B9 57 32   16 97 86 1C 4B
     B6 9E F7  ..O.n.W2....K...
4793   00E0: 6B B7 50 2D 16 CC 54 49   AB A8 8A 91 59
     0E 54 33  k.P-..TI....Y.T3
4794   00F0: AA C3 90 56 91 C7 A8 1E   A6 96 AC B6 42
     E9 55 50  ...V........B.UP
4795   0100: B2 EE 02 8D 1C F8 37 3B   77 98 A2 FD B7
     5E A8 9D  ......7;w....^..
4796   0110: D0 B9 31 79 67 F1 49 7B   C3 05 24 72 4C
     90        ..1yg.I...$rL.
4797 )
4798 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.354 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 281
4799 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.354 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
4800   0000: 0F 00 01 04 08 04 01 00   9B A2 56 31 59
     A0 53 CB  ..........V1Y.S.
4801   0010: 99 C9 64 3F FA 8E D7 E0   AD DC 36 39 D2
     0A E9 F6  ..d?......69....
4802   0020: 3D 8F 8F 4A 19 F0 AC 3F   A5 29 34 BC F0
     47 8F 88  =..J...?.)4..G..
4803   0030: 81 D9 F9 36 59 2A B6 90   2A 96 01 C4 08
```

```
4803 C8 12 D8  ...6Y*..*.......
4804   0040: 97 1A 59 81 6F 6D 8A 22   32 18 A0 A9 81
     EE 05 85  ..Y.om."2.......
4805   0050: 39 7E 55 90 F3 3C B9 7D   A3 FA BF 8B 4A
     D9 78 36  9.U..<......J.x6
4806   0060: 9B 57 E8 8F D8 1D C3 79   5A 21 81 26 FB
     F4 61 A9  .W.....yZ!.&..a.
4807   0070: A8 9B D1 16 82 2F EA B8   2A 8C 4E AE E9
     CD F0 38  ...../..*.N....8
4808   0080: AA 83 39 FD 65 CA 21 9D   96 40 21 F9 BF
     DB 88 03  ..9.e.!..@!.....
4809   0090: 1D 03 08 E4 12 42 C4 74   6E 7B 8D B3 B3
     5D D1 90  .....B.tn....]..
4810   00A0: 30 DF 21 6C AD 65 74 C2   08 C7 18 1F D0
     97 6F BA  0.!l.et.......o.
4811   00B0: 52 B2 4A 34 CC C6 3E C2   BF FF E9 F7 9F
     1A B8 54  R.J4..>........T
4812   00C0: 40 21 73 E0 FF 30 3B AF   D4 0A C7 E0 10
     EF AF 0E  @!s..0;.........
4813   00D0: 38 76 01 46 6E DC 13 F1   0A 32 35 85 03
     94 AA E6  8v.Fn....25.....
4814   00E0: FD E7 A5 1B 3C B5 65 4D   49 78 66 0A FA
     8C 02 47  ....<.eMIxf....G
4815   00F0: 12 0C 2B AB 88 E5 46 FF   A1 BE 36 EA E5
     37 C1 54  ..+...F...6..7.T
4816   0100: 4E 29 F8 1F 44 E5 9B BF
                                N)..D...
4817 )
4818 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.356 SGT|CertificateVerify.
     java:1166|Consuming CertificateVerify handshake
     message (
4819 "CertificateVerify": {
4820   "signature algorithm": rsa_pss_rsae_sha256
4821   "signature": {
4822     0000: 9B A2 56 31 59 A0 53 CB   99 C9 64 3F
     FA 8E D7 E0  ..V1Y.S...d?....
4823     0010: AD DC 36 39 D2 0A E9 F6   3D 8F 8F 4A
     19 F0 AC 3F  ..69....=..J...?
4824     0020: A5 29 34 BC F0 47 8F 88   81 D9 F9 36
     59 2A B6 90  .)4..G.....6Y*..
```

```
4825     0030: 2A 96 01 C4 08 C8 12 D8   97 1A 59 81
     6F 6D 8A 22  *.........Y.om."
4826     0040: 32 18 A0 A9 81 EE 05 85   39 7E 55 90
     F3 3C B9 7D  2.......9.U..<..
4827     0050: A3 FA BF 8B 4A D9 78 36   9B 57 E8 8F
     D8 1D C3 79  ....J.x6.W.....y
4828     0060: 5A 21 81 26 FB F4 61 A9   A8 9B D1 16
     82 2F EA B8  Z!.&..a....../..
4829     0070: 2A 8C 4E AE E9 CD F0 38   AA 83 39 FD
     65 CA 21 9D  *.N....8..9.e.!.
4830     0080: 96 40 21 F9 BF DB 88 03   1D 03 08 E4
     12 42 C4 74  .@!..........B.t
4831     0090: 6E 7B 8D B3 B3 5D D1 90   30 DF 21 6C
     AD 65 74 C2  n....]..0.!l.et.
4832     00A0: 08 C7 18 1F D0 97 6F BA   52 B2 4A 34
     CC C6 3E C2  ......o.R.J4..>.
4833     00B0: BF FF E9 F7 9F 1A B8 54   40 21 73 E0
     FF 30 3B AF  .......T@!s..0;.
4834     00C0: D4 0A C7 E0 10 EF AF 0E   38 76 01 46
     6E DC 13 F1  ........8v.Fn...
4835     00D0: 0A 32 35 85 03 94 AA E6   FD E7 A5 1B
     3C B5 65 4D  .25.........<.eM
4836     00E0: 49 78 66 0A FA 8C 02 47   12 0C 2B AB
     88 E5 46 FF  Ixf....G..+...F.
4837     00F0: A1 BE 36 EA E5 37 C1 54   4E 29 F8 1F
     44 E5 9B BF  ..6..7.TN)..D...
4838   }
4839 }
4840 )
4841 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.356 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4842   0000: 17 03 03 00 35 87 A7 44   CF A6 BD 91 07
     93 6F BB  ....5..D......o.
4843   0010: BF 9F 30 4C 2C 88 D7 1D   75 1B B8 7A 19
     AF D7 21  ..0L,...u..z...!
4844   0020: B9 3D EE 22 D0 92 C3 07   D8 83 10 3C B7
     74 4B 19  .=."........<.tK.
4845   0030: 7C 38 32 7E A6 7B B7 07   EA 45
                        .82......E
4846 )
```

```
4847 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.356 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 53
4848 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.356 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
4849   0000: 14 00 00 20 D0 98 D8 A2   A9 C1 DF 39 AD
     EA A8 2C  ... .......9...,
4850   0010: 3E F1 35 1C 2A 9C 02 4A   54 8E 4D 1A A0
     41 8F A9  >.5.*..JT.M..A..
4851   0020: E8 15 9D E1
                                                ....
4852 )
4853 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.357 SGT|Finished.java:917|
     Consuming server Finished handshake message (
4854 "Finished": {
4855   "verify data": {
4856     0000: D0 98 D8 A2 A9 C1 DF 39   AD EA A8 2C
     3E F1 35 1C  .......9...,>.5.
4857     0010: 2A 9C 02 4A 54 8E 4D 1A   A0 41 8F A9
     E8 15 9D E1  *..JT.M..A......
4858   }'}
4859 )
4860 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.357 SGT|SSLCipher.java:1870|
     KeyLimit read side: algorithm = AES/GCM/NOPADDING
     :KEYUPDATE
4861 countdown value = 137438953472
4862 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.357 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     ecdsa_secp384r1_sha384
4863 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.357 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     ecdsa_secp521r1_sha512
4864 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.357 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
```

```
4864 ed448
4865 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.357 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     rsa_pss_pss_sha384
4866 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.357 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     rsa_pss_pss_sha512
4867 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.357 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     rsa_pss_rsae_sha384
4868 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.358 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     rsa_pss_rsae_sha512
4869 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.358 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     rsa_pkcs1_sha256
4870 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.358 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     rsa_pkcs1_sha384
4871 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.358 SGT|CertificateMessage.
     java:1050|Unsupported authentication scheme:
     rsa_pkcs1_sha512
4872 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.358 SGT|X509Authentication.
     java:223|No X.509 cert selected for [EC, EdDSA,
     RSASSA-PSS, RSA]
4873 javax.net.ssl|WARNING|42|lettuce-nioEventLoop-6-1
     |2024-11-01 15:06:03.358 SGT|CertificateMessage.
     java:1087|No available authentication scheme
4874 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.358 SGT|CertificateMessage.
     java:1100|No available client authentication
     scheme
4875 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
```

```
4875 2024-11-01 15:06:03.358 SGT|CertificateMessage.
     java:1134|Produced client Certificate message (
4876 "Certificate": {
4877   "certificate_request_context": "",
4878   "certificate_list": [
4879 ]
4880 }
4881 )
4882 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.358 SGT|CertificateVerify.
     java:1093|No X.509 credentials negotiated for
     CertificateVerify
4883 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.358 SGT|Finished.java:687|
     Produced client Finished handshake message (
4884 "Finished": {
4885   "verify data": {
4886     0000: D3 8C D8 79 8E 59 19 22   33 0E C5 8B
     7C 86 71 D2  ...y.Y."3.....q.
4887     0010: E3 E3 A8 EB 10 6F BA 03   A9 6D FF E7
     D5 1C 94 8A  .....o...m......
4888   }'}
4889 )
4890 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.358 SGT|SSLCipher.java:2024|
     KeyLimit write side: algorithm = AES/GCM/
     NOPADDING:KEYUPDATE
4891 countdown value = 137438953472
4892 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.359 SGT|SSLEngineOutputRecord
     .java:530|WRITE: TLSv1.3 handshake, length = 44
4893 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.359 SGT|SSLCipher.java:2066|
     Plaintext before ENCRYPTION (
4894   0000: 0B 00 00 04 00 00 00 00   14 00 00 20 D3
     8C D8 79  ........... ...y
4895   0010: 8E 59 19 22 33 0E C5 8B   7C 86 71 D2 E3
     E3 A8 EB  .Y."3.....q.....
4896   0020: 10 6F BA 03 A9 6D FF E7   D5 1C 94 8A 16
     00 00 00  .o...m..........
4897   0030: 00 00 00 00 00 00 00 00   00 00 00 00 00
```

```
4897               ............
4898 )
4899 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.359 SGT|SSLEngineOutputRecord
     .java:551|Raw write (
4900   0000: 17 03 03 00 4D A5 B0 17   AA 27 05 11 7A
     08 57 F4  ....M....'..z.W.
4901   0010: 1A 02 E0 3F 80 EE B8 94   DF 88 5F 06 57
     2D F7 9A  ...?......_.W-..
4902   0020: F0 67 14 2B CF B4 FF 30   DC A0 F3 10 61
     36 8D BD  .g.+...0....a6..
4903   0030: 83 17 53 F7 DC 07 79 06   EB 1A 3E D6 0A
     DD 1C 61  ..S...y...>....a
4904   0040: 4B 1D F0 A5 87 B7 9F 1A   4D 20 E5 EF 44
     43 88 CC  K.......M ..DC..
4905   0050: FD BB
                                                    ..
4906 )
4907 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.360 SGT|SSLEngineOutputRecord
     .java:280|WRITE: TLSv1.3 application_data, length
      = 39
4908 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.360 SGT|SSLCipher.java:2066|
     Plaintext before ENCRYPTION (
4909   0000: 2A 33 0D 0A 24 34 0D 0A   41 55 54 48 0D
     0A 24 35  *3..$4..AUTH..$5
4910   0010: 0D 0A 61 64 6D 69 6E 0D   0A 24 38 0D 0A
     6D 61 64  ..admin..$8..mad
4911   0020: 68 75 6B 61 72 0D 0A 17   00 00 00 00 00
     00 00 00  hukar...........
4912   0030: 00 00 00 00 00 00 00 00
                                     ........
4913 )
4914 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.360 SGT|SSLEngineOutputRecord
     .java:296|Raw write (
4915   0000: 17 03 03 00 48 0B 5F 8F   38 D7 70 E5 3D
     4F B5 52  ....H._.8.p.=O.R
4916   0010: 32 DE 8C 7B 8D 61 1F C5   14 AF 64 69 7C
     EF 1D 95  2....a....di....
```

```
4917   0020: 24 38 FB 10 88 E3 5E C4   BC E2 D0 F7 74
     A9 B6 1C  $8....^.....t...
4918   0030: F1 BD 0D ED D5 DB B0 0B   82 6B E5 74 F3
     F9 C5 2C  .........k.t...,
4919   0040: B9 AA 40 61 54 F1 08 6B   2E EA C7 E5 80
                ..@aT..k.....
4920 )
4921 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.361 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4922   0000: 17 03 03 00 EA 4D 7F 5E   53 DC FE 51 E7
     E0 B2 11  .....M.^S..Q....
4923   0010: CF 6D DA F2 8F 7E 07 53   B3 07 C8 B8 62
     32 34 D5  .m.....S....b24.
4924   0020: 6A 60 F1 BB 83 13 89 3F   04 51 E2 F7 AE
     79 37 B2  j`.....?.Q...y7.
4925   0030: 8F BA 0B 85 42 FA 39 03   A9 3F 4A FE 93
     2E C6 D5  ....B.9..?J.....
4926   0040: E1 D9 9A 0A B0 E8 72 F6   2F 6A 6D EF 38
     B2 B7 C0  ......r./jm.8...
4927   0050: 91 D7 9F D5 A3 19 F0 88   15 13 EA A6 54
     AA B7 30  ............T..0
4928   0060: 7F 85 55 5C C4 F1 F5 F0   B8 B8 E1 DB 85
     32 89 97  ..U\.........2..
4929   0070: 13 A6 EC 24 40 08 AE BF   B0 A5 ED E5 B9
     92 23 D5  ...$@.........#.
4930   0080: 66 FF A5 16 B4 2C C3 EF   B6 5A 0F 6A A9
     FC A9 21  f....,...Z.j...!
4931   0090: E8 A6 0E 42 8C AF 98 4A   69 05 4A 77 5B
     77 79 E8  ...B...Ji.Jw[wy.
4932   00A0: 25 62 EB 83 9F 9D 5D 11   F2 E8 FA 99 C4
     B9 55 18  %b....].......U.
4933   00B0: 62 F6 A4 2A C9 E2 F1 1F   AB E8 BC 61 21
     AB 15 60  b..*.......a!..`
4934   00C0: 89 E1 21 B9 81 BA CC 34   A7 D3 34 7D 6D
     07 05 A9  ..!....4..4.m...
4935   00D0: F1 32 8B DE 71 8E 8E C6   BF BA 1F FF D3
     62 48 B6  .2..q........bH.
4936   00E0: 01 F1 75 14 8A AD 29 48   33 57 68 ED 0E
     43 AF     ..u...)H3Wh..C.
4937 )
```

```
4938 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.361 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 234
4939 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.362 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
4940   0000: 04 00 00 D5 00 00 01 2C   51 75 10 B7 08
     00 00 00  .......,Qu......
4941   0010: 00 00 00 00 00 00 C0 01   14 4A 23 06 10
     FB BF 2C  .........J#....,
4942   0020: BC 93 B0 5B 9B 29 DE 29   F6 AE 0A ED BA
     DA A4 C2  ...[.).).........
4943   0030: 35 7E 45 86 08 AA 4A BC   4D D4 6E 8E 0E
     D8 A1 83  5.E...J.M.n.....
4944   0040: 1D ED 41 A5 7F 00 18 B8   70 94 7D C1 4D
     4B 9C C9  ..A.....p...MK..
4945   0050: BF 61 89 48 A2 B1 66 2D   8D 68 9E F1 C7
     B4 56 4C  .a.H..f-.h....VL
4946   0060: 7A 4A 2D 41 01 97 49 01   0D 75 BE 53 26
     D4 98 49  zJ-A..I..u.S&..I
4947   0070: FF 67 4E 96 17 2F 18 0F   E7 98 CD D7 7D
     FB 84 05  .gN../..........
4948   0080: CA 35 BD 00 34 FE B5 08   F0 0F 63 98 F2
     A4 5A 50  .5..4.....c...ZP
4949   0090: 5B 1A 09 4D C6 D3 44 D0   19 07 7D 6D C5
     97 4A 7D  [..M..D....m..J.
4950   00A0: 02 15 34 F8 93 6D CE 06   C8 E7 DD 74 A1
     E8 92 A4  ..4..m.....t....
4951   00B0: CD 83 CA 99 D2 71 47 2D   E0 D7 9E A0 C4
     43 64 1D  .....qG-.....Cd.
4952   00C0: D7 7F A7 22 0B 14 3A 56   74 4F 4D 08 C6
     FE D3 9B  ..."..:VtOM.....
4953   00D0: C3 85 46 BD 21 BF 3D 00   00
                           ..F.!.=..
4954 )
4955 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.362 SGT|NewSessionTicket.java
     :567|Consuming NewSessionTicket message (
4956 "NewSessionTicket": {
4957   "ticket_lifetime"      : "300",
```

```
4958   "ticket_age_add"       : "<omitted>",
4959   "ticket_nonce"         : "0000000000000000",
4960   "ticket"               : {
4961     0000: 01 14 4A 23 06 10 FB BF   2C BC 93 B0
     5B 9B 29 DE  ..J#....,...[.).
4962     0010: 29 F6 AE 0A ED BA DA A4   C2 35 7E 45
     86 08 AA 4A  ).........5.E...J
4963     0020: BC 4D D4 6E 8E 0E D8 A1   83 1D ED 41
     A5 7F 00 18  .M.n.......A....
4964     0030: B8 70 94 7D C1 4D 4B 9C   C9 BF 61 89
     48 A2 B1 66  .p...MK...a.H..f
4965     0040: 2D 8D 68 9E F1 C7 B4 56   4C 7A 4A 2D
     41 01 97 49  -.h....VLzJ-A..I
4966     0050: 01 0D 75 BE 53 26 D4 98   49 FF 67 4E
     96 17 2F 18  ..u.S&..I.gN../.
4967     0060: 0F E7 98 CD D7 7D FB 84   05 CA 35 BD
     00 34 FE B5  .........5..4..
4968     0070: 08 F0 0F 63 98 F2 A4 5A   50 5B 1A 09
     4D C6 D3 44  ...c...ZP[..M..D
4969     0080: D0 19 07 7D 6D C5 97 4A   7D 02 15 34
     F8 93 6D CE  ....m..J...4..m.
4970     0090: 06 C8 E7 DD 74 A1 E8 92   A4 CD 83 CA
     99 D2 71 47  ....t.........qG
4971     00A0: 2D E0 D7 9E A0 C4 43 64   1D D7 7F A7
     22 0B 14 3A  -.....Cd....":.
4972     00B0: 56 74 4F 4D 08 C6 FE D3   9B C3 85 46
     BD 21 BF 3D  VtOM.......F.!.=
4973   }  "extensions"           : [
4974     <no extension>
4975   ]
4976 }
4977 )
4978 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.362 SGT|SSLSessionImpl.java:
     252|Session initialized:  Session(1730444763332|
     TLS_AES_128_GCM_SHA256)
4979 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.362 SGT|SSLEngineInputRecord.
     java:176|Raw read (
4980   0000: 17 03 03 00 EA 00 1A C4   77 84 E6 48 6B
     32 F9 03  ........w..Hk2..
```

```
4981   0010: 24 F0 45 79 A3 FE 5D E6   D8 B0 5B F0 57
     20 74 66  $.Ey..]...[.W tf
4982   0020: 17 06 67 B8 46 02 8C AA   11 43 E1 35 CE
     82 79 4D  ..g.F....C.5..yM
4983   0030: 18 92 39 01 88 5D 51 B4   02 B0 B2 88 62
     FA 28 E1  ..9..]Q.....b.(.
4984   0040: 47 7D 58 7D E3 2B 23 A1   39 57 71 DA 76
     5F C3 90  G.X..+#.9Wq.v_..
4985   0050: 2D 8E 12 D4 83 7D 69 27   56 FF CE AA A9
     DA EB 50  -.....i'V......P
4986   0060: 7C CC A1 04 59 F5 FF 91   C2 46 D3 D7 C7
     7F D4 66  ....Y....F.....f
4987   0070: 12 24 98 04 17 96 E2 5D   A3 64 A3 77 6E
     C6 2E 56  .$.....].d.wn..V
4988   0080: 7B F7 A6 0F 2A A5 4D 52   7B FE E8 DB ED
     5E D4 70  ....*.MR.....^.p
4989   0090: 9B 80 05 75 3E 70 78 67   09 CE 25 B3 BE
     BF 9B 77  ...u>pxg..%....w
4990   00A0: 67 9A 8D 94 6B F8 80 D2   C8 34 7A F8 A8
     4C 88 97  g...k....4z..L..
4991   00B0: 5D 17 6B BD 71 5F B0 4D   A4 4D 64 24 A6
     5B 24 42  ].k.q_.M.Md$.[$B
4992   00C0: 3D 3F 01 78 F6 17 0E EE   C9 6B 56 35 D9
     C2 7D 3D  =?.x.....kV5...=
4993   00D0: 70 2A A7 16 53 F8 2E 2B   2C 51 EC 05 41
     54 BD 0F  p*..S..+,Q..AT..
4994   00E0: 12 99 74 71 26 61 AB 8B   9D C0 85 DD 18
     E6 E8     ..tq&a.........
4995 )
4996 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.362 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 234
4997 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.363 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
4998   0000: 04 00 00 D5 00 00 01 2C   AF 5B 83 8B 08
     00 00 00  .......,.[......
4999   0010: 00 00 00 00 01 00 C0 01   14 4A 23 06 10
     FB BF 2C  .........J#....,
5000   0020: BC 93 B0 5B 9B 29 DE B9   6F 5D 3E A6 E8
```

```
5000 9F 70 C3  ...[.)..o]>...p.
5001   0030: 1C B6 07 F3 00 A7 39 EE   6E 64 E1 1E C0
     4B B4 E6  ......9.nd...K..
5002   0040: 0F CD 7C 83 23 BB E1 57   25 60 64 F2 4F
     5F FD 17  ....#..W%`d.O_..
5003   0050: 7A CD 24 58 41 ED 25 B6   71 F7 BD 73 A5
     B5 AD BB  z.$XA.%.q..s....
5004   0060: 7B 5C FE 13 1B D0 B6 50   6D 7D 26 B7 02
     DD 14 C6  .\.....Pm.&.....
5005   0070: 22 FA 7D 63 5F D0 67 E9   17 46 31 82 15
     A8 6E 6E  "..c_.g..F1...nn
5006   0080: C8 E4 58 F2 A9 E6 D6 88   66 81 B0 53 7A
     E6 43 13  ..X.....f..Sz.C.
5007   0090: 28 FD 84 B7 DB 50 0C 5C   AB E0 1B 29 63
     B2 EE 34  (....P.\...)c..4
5008   00A0: 11 30 51 57 AD F0 C5 63   B9 59 68 69 91
     FF 04 51  .0QW...c.Yhi...Q
5009   00B0: 4E DC B3 D0 3A 0C 81 1D   58 88 D2 AB 6D
     EB 95 07  N...:...X...m...
5010   00C0: 00 8C DD E6 B8 14 AF 3D   AF 76 A9 E5 2D
     1D 7E E7  .......=.v..-...
5011   00D0: BA 06 F4 60 39 4F EB 00   00
                           ...`9O...
5012 )
5013 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.363 SGT|NewSessionTicket.java
     :567|Consuming NewSessionTicket message (
5014 "NewSessionTicket": {
5015   "ticket_lifetime"      : "300",
5016   "ticket_age_add"       : "<omitted>",
5017   "ticket_nonce"         : "0000000000000001",
5018   "ticket"               : {
5019     0000: 01 14 4A 23 06 10 FB BF   2C BC 93 B0
     5B 9B 29 DE  ..J#....,...[.).
5020     0010: B9 6F 5D 3E A6 E8 9F 70   C3 1C B6 07
     F3 00 A7 39  .o]>...p.......9
5021     0020: EE 6E 64 E1 1E C0 4B B4   E6 0F CD 7C
     83 23 BB E1  .nd...K......#..
5022     0030: 57 25 60 64 F2 4F 5F FD   17 7A CD 24
     58 41 ED 25  W%`d.O_..z.$XA.%
5023     0040: B6 71 F7 BD 73 A5 B5 AD   BB 7B 5C FE
```

```
5023 13 1B D0 B6  .q..s.....\.....
5024     0050: 50 6D 7D 26 B7 02 DD 14   C6 22 FA 7D
     63 5F D0 67  Pm.&....."..c_.g
5025     0060: E9 17 46 31 82 15 A8 6E   6E C8 E4 58
     F2 A9 E6 D6  ..F1...nn..X....
5026     0070: 88 66 81 B0 53 7A E6 43   13 28 FD 84
     B7 DB 50 0C  .f..Sz.C.(....P.
5027     0080: 5C AB E0 1B 29 63 B2 EE   34 11 30 51
     57 AD F0 C5  \...)c..4.0QW...
5028     0090: 63 B9 59 68 69 91 FF 04   51 4E DC B3
     D0 3A 0C 81  c.Yhi...QN...:..
5029     00A0: 1D 58 88 D2 AB 6D EB 95   07 00 8C DD
     E6 B8 14 AF  .X...m..........
5030     00B0: 3D AF 76 A9 E5 2D 1D 7E   E7 BA 06 F4
     60 39 4F EB  =.v..-.....~`9O.
5031   }  "extensions"           : [
5032     <no extension>
5033   ]
5034 }
5035 )
5036 javax.net.ssl|ALL|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.363 SGT|SSLSessionImpl.java:
     252|Session initialized:  Session(1730444763332|
     TLS_AES_128_GCM_SHA256)
5037 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.363 SGT|SSLEngineInputRecord.
     java:176|Raw read (
5038   0000: 17 03 03 00 16 2C FB B1   2B D2 E0 EA 09
     FF EF 0F  .....,..+.......
5039   0010: CE 21 6E 4D E6 53 CE DA   88 A9 71
                     .!nM.S....q
5040 )
5041 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.363 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 22
5042 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.363 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
5043   0000: 2B 4F 4B 0D 0A
                                        +OK..
```

```
5044 )
5045 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.372 SGT|SSLEngineOutputRecord
     .java:280|WRITE: TLSv1.3 application_data, length
      = 50
5046 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.372 SGT|SSLCipher.java:2066|
     Plaintext before ENCRYPTION (
5047   0000: 2A 33 0D 0A 24 33 0D 0A   53 45 54 0D 0A
     24 31 31  *3..$3..SET..$11
5048   0010: 0D 0A AC ED 00 05 74 00   04 6E 61 6D 65
     0D 0A 24  ......t..name..$
5049   0020: 31 32 0D 0A AC ED 00 05   74 00 05 6D 61
     64 68 75  12......t..madhu
5050   0030: 0D 0A 17 00 00 00 00 00   00 00 00 00 00
     00 00 00  ................
5051   0040: 00 00 00
                                                  ...
5052 )
5053 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.372 SGT|SSLEngineOutputRecord
     .java:296|Raw write (
5054   0000: 17 03 03 00 53 2F 9D CF   57 C1 B6 55 E1
     6F 26 98  ....S/..W..U.o&.
5055   0010: D1 04 DE 9B 5B DB 5B 29   FD C3 3C C2 CE
     D6 50 E8  ....[.[)..<...P.
5056   0020: B6 A6 A3 8F 15 34 35 73   30 7F 1D 10 26
     0B B5 BC  .....45s0...&...
5057   0030: B6 56 A0 17 BC 06 EA 72   55 E7 78 6A D8
     22 87 E5  .V.....rU.xj."..
5058   0040: 9D 0B E6 C3 BF 9F 46 14   CA 21 4A 5B 5A
     0E 93 90  ......F..!J[Z...
5059   0050: F7 F8 06 C3 45 E2 CD 09
                                    ....E...
5060 )
5061 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.373 SGT|SSLEngineInputRecord.
     java:176|Raw read (
5062   0000: 17 03 03 00 16 5D A4 0F   67 EB B9 5A 1B
     EE 0E D4  .....]..g..Z....
5063   0010: 85 EF D3 B5 D1 D5 94 D9   D3 FF 36
```

```
5063                   ..........6
5064 )
5065 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.373 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 22
5066 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.373 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
5067   0000: 2B 4F 4B 0D 0A
                                            +OK..
5068 )
5069 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.374 SGT|SSLEngineOutputRecord
     .java:280|WRITE: TLSv1.3 application_data, length
      = 31
5070 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.374 SGT|SSLCipher.java:2066|
     Plaintext before ENCRYPTION (
5071   0000: 2A 32 0D 0A 24 33 0D 0A   47 45 54 0D 0A
     24 31 31  *2..$3..GET..$11
5072   0010: 0D 0A AC ED 00 05 74 00   04 6E 61 6D 65
     0D 0A 17  ......t..name...
5073   0020: 00 00 00 00 00 00 00 00   00 00 00 00 00
     00 00 00  ................
5074 )
5075 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.374 SGT|SSLEngineOutputRecord
     .java:296|Raw write (
5076   0000: 17 03 03 00 40 DB F9 67   9C 34 11 75 50
     F7 F1 04  ....@..g.4.uP...
5077   0010: FC 45 EC 44 F4 62 25 79   B9 DA 46 9A 4B
     1D 39 6C  .E.D.b%y..F.K.9l
5078   0020: CD 87 89 EA 9A 8D 63 BF   8B 83 2A 73 78
     B2 2F 28  ......c...*sx./(
5079   0030: 18 5D D5 B8 7F 80 79 4A   F3 D6 54 D8 B2
     26 0E 4B  .]....yJ..T..&.K
5080   0040: 5B D6 51 62 AE
                                            [.Qb.
5081 )
5082 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
```

```
5082 2024-11-01 15:06:03.374 SGT|SSLEngineInputRecord.
     java:176|Raw read (
5083   0000: 17 03 03 00 24 F0 38 EF   C5 B0 43 D9 1A
     07 F5 A9  ....$.8...C.....
5084   0010: 3D 3E BC 9B C5 B0 16 E6   1C 05 5D 84 03
     DE 75 94  =>........]...u.
5085   0020: FB 62 64 1D BF 70 3E 4E   7B
                           .bd..p>N.
5086 )
5087 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.374 SGT|SSLEngineInputRecord.
     java:213|READ: TLSv1.2 application_data, length
      = 36
5088 javax.net.ssl|DEBUG|42|lettuce-nioEventLoop-6-1|
     2024-11-01 15:06:03.374 SGT|SSLCipher.java:1961|
     Plaintext after DECRYPTION (
5089   0000: 24 31 32 0D 0A AC ED 00   05 74 00 05 6D
     61 64 68  $12......t..madh
5090   0010: 75 0D 0A
                                                u..
5091 )
5092 2024-11-01T15:06:03.375+08:00  INFO 29986 --- [
     redis-guard] [           main] i.m.r.runner.
     RedisCommandLineRunner      : The value madhu
5093
```