Hi Guys,

We are trying to access a restful web service resource hosted on IIS server with https protocol.

When we disable TWO WAY SSL Auth (server side validation of client certificate disabled) everything works fine,

When the IIS imposes TWO WAY SSL (server side validation of client certificate enabled) we are getting the below exception.

<h2>403 - Forbidden: Access is denied.</h2>

<h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>

We are using java 1.8 update 102 , IIS server 7.5 and TLS 1.2

The procedure what we followed is to import the certificates,

1. **Got the root.cer certificate from server and imported in to java client *truststore file and content as follow***

D:\ssl\26\_10>keytool -v -list -keystore truststore

Enter keystore password:

Keystore type: JKS

Keystore provider: SUN

Your keystore contains 1 entry

Alias name: ebs\_root

Creation date: Oct 26, 2017

Entry type: trustedCertEntry

Owner: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Serial number: 5e0a370ea7a758a349b2990563618d33

Valid from: Thu Aug 24 11:53:03 IST 2017 until: Wed Aug 24 12:03:02 IST 2022

Certificate fingerprints:

MD5: 8F:7E:FA:7E:9D:44:7B:D9:AF:96:45:D0:1F:E7:70:69

SHA1: 24:01:07:62:95:88:51:0B:34:D3:80:50:A3:05:20:04:05:9C:6D:14

SHA256: 5A:29:D9:59:8E:5F:3E:6D:68:CE:92:D1:78:65:16:96:49:E3:67:04:D4:5F:D7:59:E2:E0:78:63:EF:05:D3:0B

Signature algorithm name: SHA256withRSA

Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

0000: 02 01 00 ...

#2: ObjectId: 2.5.29.19 Criticality=true

BasicConstraints:[

CA:true

PathLen:2147483647

]

#3: ObjectId: 2.5.29.15 Criticality=false

KeyUsage [

DigitalSignature

Key\_CertSign

Crl\_Sign

]

#4: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 63 C1 AF AD 31 A3 7F 6E 8A F5 D2 9F 92 61 25 7B c...1..n.....a%.

0010: 88 F3 F5 52 ...R

]

]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **Downloaded the certificates from same CA server and imported into keystore file and below are the PrivateKeyEntry and trustedCertEntry inside the keystore file**

D:\ssl\26\_10>keytool -v -list -keystore keystore

Enter keystore password:

Keystore type: JKS

Keystore provider: SUN

Your keystore contains 2 entries

Alias name: ws-inblr749

Creation date: Oct 26, 2017

Entry type: PrivateKeyEntry

Certificate chain length: 1

Certificate[1]:

Owner: CN=BonusingServer, OU=IMB, O=Bally, L=Bangalore

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Serial number: 3900000131554a95f194a04ced000000000131

Valid from: Thu Oct 26 14:31:26 IST 2017 until: Fri Oct 26 14:31:26 IST 2018

Certificate fingerprints:

MD5: 0F:6B:06:16:3F:AA:AD:A6:1F:69:63:D8:1B:7F:37:15

SHA1: 05:88:B8:79:42:ED:9B:C9:1E:AE:DF:A0:65:3F:68:FE:73:66:0F:31

SHA256: EB:02:2B:8D:42:51:48:B0:3E:05:06:D1:55:B1:7A:AC:45:1E:34:22:E0:3E:58:10:7A:1B:08:56:B6:AE:9F:0C

Signature algorithm name: SHA256withRSA

Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false

0000: 30 26 30 0C 06 0A 2B 06 01 04 01 82 37 14 02 02 0&0...+.....7...

0010: 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 06 08 0...+.......0...

0020: 2B 06 01 05 05 07 03 02 +.......

#2: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false

0000: 30 2E 06 26 2B 06 01 04 01 82 37 15 08 86 A3 96 0..&+.....7.....

0010: 13 85 E6 A6 4E 99 99 2D 82 B3 A4 3F 82 B5 F8 25 ....N..-...?...%

0020: 81 07 81 B8 8E 3C 83 CC 91 34 02 01 64 02 01 08 .....<...4..d...

#3: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false

AuthorityInfoAccess [

[

accessMethod: caIssuers

accessLocation: URIName: ldap:///CN=EBS-WIN-0SNCU0GA0AM-CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=EBS,DC=QA?cACertificate?base?objectClass=certificationAuthority

]

]

#4: ObjectId: 2.5.29.35 Criticality=false

AuthorityKeyIdentifier [

KeyIdentifier [

0000: 63 C1 AF AD 31 A3 7F 6E 8A F5 D2 9F 92 61 25 7B c...1..n.....a%.

0010: 88 F3 F5 52 ...R

]

]

#5: ObjectId: 2.5.29.31 Criticality=false

CRLDistributionPoints [

[DistributionPoint:

[URIName: ldap:///CN=EBS-WIN-0SNCU0GA0AM-CA,CN=WIN-0SNCU0GA0AM,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=EBS,DC=QA?certificateRevocationList?base?objectClass=cRLDistributionPoint]

]]

#6: ObjectId: 2.5.29.37 Criticality=false

ExtendedKeyUsages [

1.3.6.1.4.1.311.20.2.2

serverAuth

clientAuth

]

#7: ObjectId: 2.5.29.15 Criticality=true

KeyUsage [

DigitalSignature

Key\_Encipherment

]

#8: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: WS-INBLR749.ad.agi

DNSName: localhost

DNSName: 10.2.200.166

IPAddress: 10.2.200.166

DNSName: BonusingServer

]

#9: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 62 89 70 9E A0 02 8A 58 BB 62 39 70 6C 77 9D 99 b.p....X.b9plw..

0010: 7C F4 FA B7 ....

]

]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Alias name: root\_sds

Creation date: Oct 26, 2017

Entry type: trustedCertEntry

Owner: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Serial number: 5e0a370ea7a758a349b2990563618d33

Valid from: Thu Aug 24 11:53:03 IST 2017 until: Wed Aug 24 12:03:02 IST 2022

Certificate fingerprints:

MD5: 8F:7E:FA:7E:9D:44:7B:D9:AF:96:45:D0:1F:E7:70:69

SHA1: 24:01:07:62:95:88:51:0B:34:D3:80:50:A3:05:20:04:05:9C:6D:14

SHA256: 5A:29:D9:59:8E:5F:3E:6D:68:CE:92:D1:78:65:16:96:49:E3:67:04:D4:5F:D7:59:E2:E0:78:63:EF:05:D3:0B

Signature algorithm name: SHA256withRSA

Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

0000: 02 01 00 ...

#2: ObjectId: 2.5.29.19 Criticality=true

BasicConstraints:[

CA:true

PathLen:2147483647

]

#3: ObjectId: 2.5.29.15 Criticality=false

KeyUsage [

DigitalSignature

Key\_CertSign

Crl\_Sign

]

#4: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 63 C1 AF AD 31 A3 7F 6E 8A F5 D2 9F 92 61 25 7B c...1..n.....a%.

0010: 88 F3 F5 52 ...R

]

]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **Below is our java client code**

import java.io.BufferedReader;  
import java.io.IOException;

import java.io.InputStreamReader;

import org.apache.http.HttpResponse;

import org.apache.http.client.ClientProtocolException;

import org.apache.http.client.HttpClient;

import org.apache.http.client.methods.HttpPost;

import org.apache.http.impl.client.HttpClientBuilder;

System.setProperty("javax.net.debug", "ssl");

System.setProperty("javax.net.ssl.keyStoreType", "jks");

System.setProperty("javax.net.ssl.keyStore", "D:/ssl/26\_10/keystore");

System.setProperty("javax.net.ssl.keyStorePassword","changeit");

System.setProperty("javax.net.ssl.trustStoreType","jks");

System.setProperty("javax.net.ssl.trustStore", "D:/ssl/26\_10/truststore");

System.setProperty("javax.net.ssl.trustStorePassword", "changeit");

try {

StringBuffer stringBuffer = new StringBuffer();

HttpClient client = HttpClientBuilder.create().build();

String urlStr = "https://IIS\_SERVR\_IP:PORT/EBSMeterDataManagement/api/v1/MeterDataExchange/MeterTransactionsBySiteId/512/1505470085920/1510470647610";

HttpGet request = new HttpGet(urlStr);

request.addHeader("accept", "application/json");

request.addHeader("x-api-key","40-C3-48-C0-01-06-8C-FB-40-9A-73-CF-94-E8-59-D4-90-E5-A7-2A-0C-0D-03-71-72-F1-61-76-64-28-D8-F5");

HttpResponse response = client.execute(request);

BufferedReader br = new BufferedReader(new InputStreamReader((response.getEntity().getContent())));

String output = "";

while ((output = br.readLine()) != null) {

stringBuffer.append(output);

}

System.out.println(stringBuffer);

} catch (ClientProtocolException e) {

// TODO Auto-generated catch block

e.printStackTrace();

} catch (IOException e) {

// TODO Auto-generated catch block

e.printStackTrace();

}

1. **Below is the SSL debug logger**

trustStore is: D:\ssl\26\_10\truststore

trustStore type is : jks

trustStore provider is :

init truststore

adding as trusted cert:

Subject: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Algorithm: RSA; Serial number: 0x5e0a370ea7a758a349b2990563618d33

Valid from Thu Aug 24 11:53:03 IST 2017 until Wed Aug 24 12:03:02 IST 2022

trigger seeding of SecureRandom

done seeding SecureRandom

Ignoring unavailable cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384

Ignoring unavailable cipher suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

Ignoring unavailable cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Ignoring unavailable cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA

Ignoring unavailable cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

Ignoring unavailable cipher suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

Ignoring unavailable cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA

Ignoring unavailable cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

Ignoring unavailable cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384

Ignoring unavailable cipher suite: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Ignoring unavailable cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384

Ignoring unavailable cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384

Ignoring unavailable cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA

Ignoring unavailable cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Ignoring unavailable cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384

Ignoring unavailable cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256

Ignoring unavailable cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA

Ignoring unavailable cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256

Ignoring unavailable cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Ignoring unavailable cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Ignoring unavailable cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Allow unsafe renegotiation: false

Allow legacy hello messages: true

Is initial handshake: true

Is secure renegotiation: false

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

%% No cached client session

\*\*\* ClientHello, TLSv1.2

RandomCookie: GMT: 1492178583 bytes = { 151, 212, 45, 1, 112, 65, 217, 166, 92, 188, 80, 221, 213, 37, 173, 138, 9, 126, 203, 41, 117, 172, 240, 143, 80, 125, 197, 128 }

Session ID: {}

Cipher Suites: [TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV]

Compression Methods: { 0 }

Extension elliptic\_curves, curve names: {secp256r1, sect163k1, sect163r2, secp192r1, secp224r1, sect233k1, sect233r1, sect283k1, sect283r1, secp384r1, sect409k1, sect409r1, secp521r1, sect571k1, sect571r1, secp160k1, secp160r1, secp160r2, sect163r1, secp192k1, sect193r1, sect193r2, secp224k1, sect239k1, secp256k1}

Extension ec\_point\_formats, formats: [uncompressed]

Extension signature\_algorithms, signature\_algorithms: SHA512withECDSA, SHA512withRSA, SHA384withECDSA, SHA384withRSA, SHA256withECDSA, SHA256withRSA, SHA1withECDSA, SHA1withRSA, SHA1withDSA

\*\*\*

main, WRITE: TLSv1.2 Handshake, length = 189

main, READ: TLSv1.2 Handshake, length = 1680

\*\*\* ServerHello, TLSv1.2

RandomCookie: GMT: 1492178583 bytes = { 121, 8, 67, 125, 11, 124, 182, 112, 187, 135, 8, 34, 212, 63, 197, 113, 238, 83, 68, 161, 137, 115, 112, 51, 173, 170, 200, 160 }

Session ID: {250, 51, 0, 0, 165, 113, 200, 82, 108, 73, 188, 219, 124, 193, 135, 123, 196, 120, 67, 240, 230, 77, 31, 62, 96, 153, 42, 66, 150, 232, 91, 2}

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Compression Method: 0

Extension renegotiation\_info, renegotiated\_connection: <empty>

\*\*\*

%% Initialized: [Session-1, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

\*\* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

\*\*\* Certificate chain

chain [0] = [

[

Version: V3

Subject: CN=BonusingServer, OU=IMB, O=Bally, L=Bangalore

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 17340031878443709349087149953464484513683672003734036519468571340040626601021461243449639227265153392322165167563204542447619887538196148558361157158439718674368290164513532754771734171756637123248694905570623218070820581037224673105951696373241110008125883365350963675774476157410039454450807034402338212700348308377619493242495297307380301814392000905327006160593819150382739588792981901765981401985511363323787093139696294876276576980199368010742599663574272030806176499739419093827838768479591842834177115319787473321723562488729355729897272454619343665282403163311785820219068782813379418895566709025579812409447

public exponent: 65537

Validity: [From: Thu Oct 26 13:56:24 IST 2017,

To: Fri Oct 26 13:56:24 IST 2018]

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

SerialNumber: [ 39000001 308c6583 d9ae818d 4f000000 000130]

Certificate Extensions: 9

[1]: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false

Extension unknown: DER encoded OCTET string =

0000: 04 28 30 26 30 0C 06 0A 2B 06 01 04 01 82 37 14 .(0&0...+.....7.

0010: 02 02 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A ..0...+.......0.

0020: 06 08 2B 06 01 05 05 07 03 02 ..+.......

[2]: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false

Extension unknown: DER encoded OCTET string =

0000: 04 30 30 2E 06 26 2B 06 01 04 01 82 37 15 08 86 .00..&+.....7...

0010: A3 96 13 85 E6 A6 4E 99 99 2D 82 B3 A4 3F 82 B5 ......N..-...?..

0020: F8 25 81 07 81 B8 8E 3C 83 CC 91 34 02 01 64 02 .%.....<...4..d.

0030: 01 08 ..

[3]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false

AuthorityInfoAccess [

[

accessMethod: caIssuers

accessLocation: URIName: ldap:///CN=EBS-WIN-0SNCU0GA0AM-CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=EBS,DC=QA?cACertificate?base?objectClass=certificationAuthority

]

]

[4]: ObjectId: 2.5.29.35 Criticality=false

AuthorityKeyIdentifier [

KeyIdentifier [

0000: 63 C1 AF AD 31 A3 7F 6E 8A F5 D2 9F 92 61 25 7B c...1..n.....a%.

0010: 88 F3 F5 52 ...R

]

]

[5]: ObjectId: 2.5.29.31 Criticality=false

CRLDistributionPoints [

[DistributionPoint:

[URIName: ldap:///CN=EBS-WIN-0SNCU0GA0AM-CA,CN=WIN-0SNCU0GA0AM,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=EBS,DC=QA?certificateRevocationList?base?objectClass=cRLDistributionPoint]

]]

[6]: ObjectId: 2.5.29.37 Criticality=false

ExtendedKeyUsages [

1.3.6.1.4.1.311.20.2.2

serverAuth

clientAuth

]

[7]: ObjectId: 2.5.29.15 Criticality=true

KeyUsage [

DigitalSignature

Key\_Encipherment

]

[8]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: DT-7YRW8R1.ad.agi

DNSName: localhost

DNSName: 10.2.142.57

IPAddress: 10.2.142.57

DNSName: 192.168.56.1

IPAddress: 192.168.56.1

DNSName: 192.168.69.2

IPAddress: 192.168.69.2

DNSName: BonusingServer

]

[9]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 33 D6 94 DD 75 86 94 D8 70 56 8F B4 7C 75 30 8B 3...u...pV...u0.

0010: 4F DC 35 F9 O.5.

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 4E E0 5A 3E 9D A6 47 64 42 EB 4E BF 1E 34 B3 C9 N.Z>..GdB.N..4..

0010: C3 06 0C E1 BE 78 C8 4E 23 36 18 DD 26 FD E4 CC .....x.N#6..&...

0020: 50 16 0F 74 EF 27 22 00 7D 40 41 0A 9E B0 3D D3 P..t.'"..@A...=.

0030: 02 99 9F 18 AE 9C 27 CB E8 9D 8B 90 88 1F 12 7A ......'........z

0040: C8 74 6A 38 C7 F1 D1 4A 1C BB 88 51 79 3A 9C 73 .tj8...J...Qy:.s

0050: 81 67 12 E6 F1 69 C8 99 0C AB B0 CC 7E 22 DB 9F .g...i......."..

0060: 89 46 41 70 6F B4 D9 88 34 3A A3 33 EC 03 E3 B1 .FApo...4:.3....

0070: 25 4F 85 AC F7 36 8C C7 36 C3 77 48 11 89 8A 5A %O...6..6.wH...Z

0080: EC 05 BC BB E1 79 17 C4 52 D2 F3 B2 CD F2 3E 82 .....y..R.....>.

0090: 60 79 A0 FD CA D3 95 44 F2 EF 61 B0 DC 87 2A 23 `y.....D..a...\*#

00A0: 75 EF 7D 98 56 FC 1A 5C D9 2B C1 BC CC E0 AB 06 u...V..\.+......

00B0: E2 8A 74 E4 F5 92 A1 22 98 18 AC 36 24 32 2B 7D ..t...."...6$2+.

00C0: C6 6D E6 E7 63 69 B0 D0 16 E3 36 EF 3D 28 B8 6E .m..ci....6.=(.n

00D0: E7 E0 04 1D 40 8F 31 07 02 D0 A9 70 3D 42 76 EC ....@.1....p=Bv.

00E0: B9 FB B8 98 55 B4 2A 48 D9 1E 25 25 AC 87 5E 7E ....U.\*H..%%..^.

00F0: 18 7E F6 51 EA DD 76 5A 02 33 BE 46 98 B4 10 CA ...Q..vZ.3.F....

]

\*\*\*

Found trusted certificate:

[

[

Version: V3

Subject: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 28860036678669032106011003029844459822942026122785728670484243710324781404355493427120054209353824603303779852422542951306180543993440671225422502368505469453647312738967265459740813093390760508557444158215818619038555192615652573450172830946489701857746205818898503000752601467573154656255824824865981661400178389137848940460400335782830110323238710939787001119089994189135501648345679449984381290800571945550910777021844098277222282503316146047163290028267080564930960783671210054240569746966504181270972094082745399131207273769674360056131041948547695038077792603317911002220541179024713269547572635764945286105493

public exponent: 65537

Validity: [From: Thu Aug 24 11:53:03 IST 2017,

To: Wed Aug 24 12:03:02 IST 2022]

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

SerialNumber: [ 5e0a370e a7a758a3 49b29905 63618d33]

Certificate Extensions: 4

[1]: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

Extension unknown: DER encoded OCTET string =

0000: 04 03 02 01 00 .....

[2]: ObjectId: 2.5.29.19 Criticality=true

BasicConstraints:[

CA:true

PathLen:2147483647

]

[3]: ObjectId: 2.5.29.15 Criticality=false

KeyUsage [

DigitalSignature

Key\_CertSign

Crl\_Sign

]

[4]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 63 C1 AF AD 31 A3 7F 6E 8A F5 D2 9F 92 61 25 7B c...1..n.....a%.

0010: 88 F3 F5 52 ...R

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 07 44 3A 38 4C 8C 9D 66 68 67 01 56 91 CA 77 71 .D:8L..fhg.V..wq

0010: 84 8B 4A AA 73 5C 85 4F 19 AC 09 C6 38 D1 5B D0 ..J.s\.O....8.[.

0020: C5 6B 98 DD C4 DC 40 8C 67 FC 63 B9 D0 54 28 EF .k....@.g.c..T(.

0030: 18 92 66 C3 08 ED 55 2D 39 DC 61 DA A5 11 79 EE ..f...U-9.a...y.

0040: 6A 36 81 C4 C6 34 45 68 5E 4C E5 24 E7 7E 35 C7 j6...4Eh^L.$..5.

0050: C0 A7 89 93 1B F5 8F C8 80 C5 F4 E3 DC 0B B4 3C ...............<

0060: 7D 5E 36 6D 8C D6 3F 53 F6 80 22 AC D6 8D B6 D1 .^6m..?S..".....

0070: A6 AB 6C A5 27 19 27 24 07 8B D6 33 4C 0F 91 55 ..l.'.'$...3L..U

0080: F6 58 54 AE 96 80 13 C3 CF 7A D6 A5 CB BC 2E AF .XT......z......

0090: E7 4A B5 1B B1 37 63 B7 DD C5 9E 1E CA 41 7E 2B .J...7c......A.+

00A0: A0 5C 40 20 78 FA 01 4A 07 8F 22 A2 D1 E5 DA 0B .\@ x..J..".....

00B0: 10 CA C4 B4 20 0B 60 A7 74 CB 4F AF 71 1B EC 75 .... .`.t.O.q..u

00C0: C5 68 9E 0E 00 5C 7E D5 B8 08 51 19 00 8C 9E C5 .h...\....Q.....

00D0: 8C 20 3D 44 BB 42 49 D7 E0 65 B6 77 5D CE AA 09 . =D.BI..e.w]...

00E0: D4 43 16 C5 8E 7F FF 54 EE 6A EA B5 03 41 A1 8A .C.....T.j...A..

00F0: 81 35 6A FB 8E A0 66 07 A1 99 23 37 AA 94 AD 6F .5j...f...#7...o

]

\*\*\* ServerHelloDone

\*\*\* ClientKeyExchange, RSA PreMasterSecret, TLSv1.2

main, WRITE: TLSv1.2 Handshake, length = 262

SESSION KEYGEN:

PreMaster Secret:

0000: 03 03 C6 B9 9B C8 C3 10 79 B8 84 EF 9B 37 1A 9C ........y....7..

0010: A1 F3 80 73 97 EC 95 04 62 D9 0B 85 C1 E4 6C 86 ...s....b.....l.

0020: 5A 68 38 B5 96 A3 34 4B A8 D0 7D 48 55 47 68 6D Zh8...4K...HUGhm

CONNECTION KEYGEN:

Client Nonce:

0000: 59 F1 D7 97 97 D4 2D 01 70 41 D9 A6 5C BC 50 DD Y.....-.pA..\.P.

0010: D5 25 AD 8A 09 7E CB 29 75 AC F0 8F 50 7D C5 80 .%.....)u...P...

Server Nonce:

0000: 59 F1 D7 97 79 08 43 7D 0B 7C B6 70 BB 87 08 22 Y...y.C....p..."

0010: D4 3F C5 71 EE 53 44 A1 89 73 70 33 AD AA C8 A0 .?.q.SD..sp3....

Master Secret:

0000: BE ED 51 98 8E 36 47 BA 97 0F 90 61 0E AC F7 55 ..Q..6G....a...U

0010: 68 4F EF F7 5B 4A 09 19 F4 6D 4E C7 01 92 C4 84 hO..[J...mN.....

0020: 6F 47 B4 61 F5 80 85 31 31 FB 8F 6E 70 F3 75 79 oG.a...11..np.uy

Client MAC write Secret:

0000: 90 99 02 22 73 AD EB 7D 91 19 7E 9B 3D 83 D7 1F ..."s.......=...

0010: 6E D9 4E C1 7E 9F 49 E7 73 DD 78 EC 8D 24 C5 7F n.N...I.s.x..$..

Server MAC write Secret:

0000: 0F 5B C2 57 AD C1 67 A7 28 AC A1 A0 0D B1 F9 73 .[.W..g.(......s

0010: 92 26 C4 D2 48 5E 10 A5 62 4D 9B 66 50 E9 23 DD .&..H^..bM.fP.#.

Client write key:

0000: F3 2F 73 85 44 53 E4 7B 6D C3 72 D9 90 08 66 55 ./s.DS..m.r...fU

Server write key:

0000: 65 E2 7B B4 31 B8 C3 0F D2 BC D5 AF E4 F8 62 EE e...1.........b.

... no IV derived for this protocol

main, WRITE: TLSv1.2 Change Cipher Spec, length = 1

\*\*\* Finished

verify\_data: { 41, 248, 129, 108, 69, 235, 78, 246, 184, 72, 19, 42 }

\*\*\*

main, WRITE: TLSv1.2 Handshake, length = 80

main, READ: TLSv1.2 Change Cipher Spec, length = 1

main, READ: TLSv1.2 Handshake, length = 80

\*\*\* Finished

verify\_data: { 115, 200, 22, 225, 113, 249, 34, 79, 9, 66, 185, 109 }

\*\*\*

%% Cached client session: [Session-1, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

main, WRITE: TLSv1.2 Application Data, length = 288

main, READ: TLSv1.2 Handshake, length = 64

Allow unsafe renegotiation: false

Allow legacy hello messages: true

Is initial handshake: false

Is secure renegotiation: true

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1

Ignoring unsupported cipher suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

Ignoring unsupported cipher suite: TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 for TLSv1.1

\*\*\* HelloRequest (empty)

%% Client cached [Session-1, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

%% Try resuming [Session-1, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256] from port 63606

\*\*\* ClientHello, TLSv1.2

RandomCookie: GMT: 1492178583 bytes = { 132, 251, 3, 72, 208, 107, 163, 35, 49, 142, 11, 22, 114, 187, 29, 232, 215, 106, 10, 50, 64, 218, 17, 117, 210, 98, 27, 240 }

Session ID: {250, 51, 0, 0, 165, 113, 200, 82, 108, 73, 188, 219, 124, 193, 135, 123, 196, 120, 67, 240, 230, 77, 31, 62, 96, 153, 42, 66, 150, 232, 91, 2}

Cipher Suites: [TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA]

Compression Methods: { 0 }

Extension elliptic\_curves, curve names: {secp256r1, sect163k1, sect163r2, secp192r1, secp224r1, sect233k1, sect233r1, sect283k1, sect283r1, secp384r1, sect409k1, sect409r1, secp521r1, sect571k1, sect571r1, secp160k1, secp160r1, secp160r2, sect163r1, secp192k1, sect193r1, sect193r2, secp224k1, sect239k1, secp256k1}

Extension ec\_point\_formats, formats: [uncompressed]

Extension signature\_algorithms, signature\_algorithms: SHA512withECDSA, SHA512withRSA, SHA384withECDSA, SHA384withRSA, SHA256withECDSA, SHA256withRSA, SHA1withECDSA, SHA1withRSA, SHA1withDSA

Extension renegotiation\_info, renegotiated\_connection: 29:f8:81:6c:45:eb:4e:f6:b8:48:13:2a

\*\*\*

main, WRITE: TLSv1.2 Handshake, length = 288

main, READ: TLSv1.2 Handshake, length = 7904

\*\*\* ServerHello, TLSv1.2

RandomCookie: GMT: 1492178583 bytes = { 137, 2, 125, 49, 198, 219, 129, 143, 46, 202, 176, 234, 122, 62, 12, 203, 245, 98, 2, 197, 245, 22, 250, 224, 127, 119, 167, 107 }

Session ID: {69, 70, 0, 0, 242, 190, 6, 236, 15, 12, 225, 243, 61, 200, 68, 184, 123, 99, 222, 12, 14, 80, 255, 150, 228, 30, 252, 201, 64, 135, 204, 224}

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Compression Method: 0

Extension renegotiation\_info, renegotiated\_connection: 29:f8:81:6c:45:eb:4e:f6:b8:48:13:2a:73:c8:16:e1:71:f9:22:4f:09:42:b9:6d

\*\*\*

%% Invalidated: [Session-1, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

%% Initialized: [Session-2, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

\*\* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

\*\*\* Certificate chain

chain [0] = [

[

Version: V3

Subject: CN=BonusingServer, OU=IMB, O=Bally, L=Bangalore

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 17340031878443709349087149953464484513683672003734036519468571340040626601021461243449639227265153392322165167563204542447619887538196148558361157158439718674368290164513532754771734171756637123248694905570623218070820581037224673105951696373241110008125883365350963675774476157410039454450807034402338212700348308377619493242495297307380301814392000905327006160593819150382739588792981901765981401985511363323787093139696294876276576980199368010742599663574272030806176499739419093827838768479591842834177115319787473321723562488729355729897272454619343665282403163311785820219068782813379418895566709025579812409447

public exponent: 65537

Validity: [From: Thu Oct 26 13:56:24 IST 2017,

To: Fri Oct 26 13:56:24 IST 2018]

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

SerialNumber: [ 39000001 308c6583 d9ae818d 4f000000 000130]

Certificate Extensions: 9

[1]: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false

Extension unknown: DER encoded OCTET string =

0000: 04 28 30 26 30 0C 06 0A 2B 06 01 04 01 82 37 14 .(0&0...+.....7.

0010: 02 02 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A ..0...+.......0.

0020: 06 08 2B 06 01 05 05 07 03 02 ..+.......

[2]: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false

Extension unknown: DER encoded OCTET string =

0000: 04 30 30 2E 06 26 2B 06 01 04 01 82 37 15 08 86 .00..&+.....7...

0010: A3 96 13 85 E6 A6 4E 99 99 2D 82 B3 A4 3F 82 B5 ......N..-...?..

0020: F8 25 81 07 81 B8 8E 3C 83 CC 91 34 02 01 64 02 .%.....<...4..d.

0030: 01 08 ..

[3]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false

AuthorityInfoAccess [

[

accessMethod: caIssuers

accessLocation: URIName: ldap:///CN=EBS-WIN-0SNCU0GA0AM-CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=EBS,DC=QA?cACertificate?base?objectClass=certificationAuthority

]

]

[4]: ObjectId: 2.5.29.35 Criticality=false

AuthorityKeyIdentifier [

KeyIdentifier [

0000: 63 C1 AF AD 31 A3 7F 6E 8A F5 D2 9F 92 61 25 7B c...1..n.....a%.

0010: 88 F3 F5 52 ...R

]

]

[5]: ObjectId: 2.5.29.31 Criticality=false

CRLDistributionPoints [

[DistributionPoint:

[URIName: ldap:///CN=EBS-WIN-0SNCU0GA0AM-CA,CN=WIN-0SNCU0GA0AM,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=EBS,DC=QA?certificateRevocationList?base?objectClass=cRLDistributionPoint]

]]

[6]: ObjectId: 2.5.29.37 Criticality=false

ExtendedKeyUsages [

1.3.6.1.4.1.311.20.2.2

serverAuth

clientAuth

]

[7]: ObjectId: 2.5.29.15 Criticality=true

KeyUsage [

DigitalSignature

Key\_Encipherment

]

[8]: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

DNSName: DT-7YRW8R1.ad.agi

DNSName: localhost

DNSName: 10.2.142.57

IPAddress: 10.2.142.57

DNSName: 192.168.56.1

IPAddress: 192.168.56.1

DNSName: 192.168.69.2

IPAddress: 192.168.69.2

DNSName: BonusingServer

]

[9]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 33 D6 94 DD 75 86 94 D8 70 56 8F B4 7C 75 30 8B 3...u...pV...u0.

0010: 4F DC 35 F9 O.5.

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 4E E0 5A 3E 9D A6 47 64 42 EB 4E BF 1E 34 B3 C9 N.Z>..GdB.N..4..

0010: C3 06 0C E1 BE 78 C8 4E 23 36 18 DD 26 FD E4 CC .....x.N#6..&...

0020: 50 16 0F 74 EF 27 22 00 7D 40 41 0A 9E B0 3D D3 P..t.'"..@A...=.

0030: 02 99 9F 18 AE 9C 27 CB E8 9D 8B 90 88 1F 12 7A ......'........z

0040: C8 74 6A 38 C7 F1 D1 4A 1C BB 88 51 79 3A 9C 73 .tj8...J...Qy:.s

0050: 81 67 12 E6 F1 69 C8 99 0C AB B0 CC 7E 22 DB 9F .g...i......."..

0060: 89 46 41 70 6F B4 D9 88 34 3A A3 33 EC 03 E3 B1 .FApo...4:.3....

0070: 25 4F 85 AC F7 36 8C C7 36 C3 77 48 11 89 8A 5A %O...6..6.wH...Z

0080: EC 05 BC BB E1 79 17 C4 52 D2 F3 B2 CD F2 3E 82 .....y..R.....>.

0090: 60 79 A0 FD CA D3 95 44 F2 EF 61 B0 DC 87 2A 23 `y.....D..a...\*#

00A0: 75 EF 7D 98 56 FC 1A 5C D9 2B C1 BC CC E0 AB 06 u...V..\.+......

00B0: E2 8A 74 E4 F5 92 A1 22 98 18 AC 36 24 32 2B 7D ..t...."...6$2+.

00C0: C6 6D E6 E7 63 69 B0 D0 16 E3 36 EF 3D 28 B8 6E .m..ci....6.=(.n

00D0: E7 E0 04 1D 40 8F 31 07 02 D0 A9 70 3D 42 76 EC ....@.1....p=Bv.

00E0: B9 FB B8 98 55 B4 2A 48 D9 1E 25 25 AC 87 5E 7E ....U.\*H..%%..^.

00F0: 18 7E F6 51 EA DD 76 5A 02 33 BE 46 98 B4 10 CA ...Q..vZ.3.F....

]

\*\*\*

Found trusted certificate:

[

[

Version: V3

Subject: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits

modulus: 28860036678669032106011003029844459822942026122785728670484243710324781404355493427120054209353824603303779852422542951306180543993440671225422502368505469453647312738967265459740813093390760508557444158215818619038555192615652573450172830946489701857746205818898503000752601467573154656255824824865981661400178389137848940460400335782830110323238710939787001119089994189135501648345679449984381290800571945550910777021844098277222282503316146047163290028267080564930960783671210054240569746966504181270972094082745399131207273769674360056131041948547695038077792603317911002220541179024713269547572635764945286105493

public exponent: 65537

Validity: [From: Thu Aug 24 11:53:03 IST 2017,

To: Wed Aug 24 12:03:02 IST 2022]

Issuer: CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA

SerialNumber: [ 5e0a370e a7a758a3 49b29905 63618d33]

Certificate Extensions: 4

[1]: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

Extension unknown: DER encoded OCTET string =

0000: 04 03 02 01 00 .....

[2]: ObjectId: 2.5.29.19 Criticality=true

BasicConstraints:[

CA:true

PathLen:2147483647

]

[3]: ObjectId: 2.5.29.15 Criticality=false

KeyUsage [

DigitalSignature

Key\_CertSign

Crl\_Sign

]

[4]: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 63 C1 AF AD 31 A3 7F 6E 8A F5 D2 9F 92 61 25 7B c...1..n.....a%.

0010: 88 F3 F5 52 ...R

]

]

]

Algorithm: [SHA256withRSA]

Signature:

0000: 07 44 3A 38 4C 8C 9D 66 68 67 01 56 91 CA 77 71 .D:8L..fhg.V..wq

0010: 84 8B 4A AA 73 5C 85 4F 19 AC 09 C6 38 D1 5B D0 ..J.s\.O....8.[.

0020: C5 6B 98 DD C4 DC 40 8C 67 FC 63 B9 D0 54 28 EF .k....@.g.c..T(.

0030: 18 92 66 C3 08 ED 55 2D 39 DC 61 DA A5 11 79 EE ..f...U-9.a...y.

0040: 6A 36 81 C4 C6 34 45 68 5E 4C E5 24 E7 7E 35 C7 j6...4Eh^L.$..5.

0050: C0 A7 89 93 1B F5 8F C8 80 C5 F4 E3 DC 0B B4 3C ...............<

0060: 7D 5E 36 6D 8C D6 3F 53 F6 80 22 AC D6 8D B6 D1 .^6m..?S..".....

0070: A6 AB 6C A5 27 19 27 24 07 8B D6 33 4C 0F 91 55 ..l.'.'$...3L..U

0080: F6 58 54 AE 96 80 13 C3 CF 7A D6 A5 CB BC 2E AF .XT......z......

0090: E7 4A B5 1B B1 37 63 B7 DD C5 9E 1E CA 41 7E 2B .J...7c......A.+

00A0: A0 5C 40 20 78 FA 01 4A 07 8F 22 A2 D1 E5 DA 0B .\@ x..J..".....

00B0: 10 CA C4 B4 20 0B 60 A7 74 CB 4F AF 71 1B EC 75 .... .`.t.O.q..u

00C0: C5 68 9E 0E 00 5C 7E D5 B8 08 51 19 00 8C 9E C5 .h...\....Q.....

00D0: 8C 20 3D 44 BB 42 49 D7 E0 65 B6 77 5D CE AA 09 . =D.BI..e.w]...

00E0: D4 43 16 C5 8E 7F FF 54 EE 6A EA B5 03 41 A1 8A .C.....T.j...A..

00F0: 81 35 6A FB 8E A0 66 07 A1 99 23 37 AA 94 AD 6F .5j...f...#7...o

]

\*\*\* CertificateRequest

Cert Types: RSA, DSS, ECDSA

Supported Signature Algorithms: SHA256withRSA, SHA384withRSA, SHA1withRSA, SHA256withECDSA, SHA384withECDSA, SHA1withECDSA, SHA1withDSA

Cert Authorities:

<CN=ad01, DC=ad, DC=agi>

<CN=ca, DC=ad, DC=agi>

<CN=Scientific Games Corporation Root CA, O=Scientific Games Corp, C=US>

<OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US>

<CN=Forcepoint Cloud CA, O=Forcepoint LLC, L=Austin, ST=Texas, C=US>

<C=US, L=San Diego, CN=Websense Inc., OU=Websense Internet Authority>

<CN=ad-LV-CA01-CA, DC=ad, DC=agi>

<CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE>

<CN=GeoTrust Primary Certification Authority - G3, OU=(c) 2008 GeoTrust Inc. - For authorized use only, O=GeoTrust Inc., C=US>

<CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US>

<CN=Certum Trusted Network CA, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL>

<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>

<CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES>

<CN=GeoTrust Primary Certification Authority, O=GeoTrust Inc., C=US>

<CN=VeriSign Universal Root Certification Authority, OU="(c) 2008 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US>

<OU=Security Communication RootCA1, O=SECOM Trust.net, C=JP>

<CN=StartCom Certification Authority, OU=Secure Digital Certificate Signing, O=StartCom Ltd., C=IL>

<CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US>

<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>

<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>

<CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US>

<CN=Certum CA, O=Unizeto Sp. z o.o., C=PL>

<OU=ePKI Root Certification Authority, O="Chunghwa Telecom Co., Ltd.", C=TW>

<CN=Class 2 Primary CA, O=Certplus, C=FR>

<OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US>

<CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2>

<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>

<CN=SecureTrust CA, O=SecureTrust Corporation, C=US>

<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>

<CN=thawte Primary Root CA, OU="(c) 2006 thawte, Inc. - For authorized use only", OU=Certification Services Division, O="thawte, Inc.", C=US>

<CN=GTE CyberTrust Global Root, OU="GTE CyberTrust Solutions, Inc.", O=GTE Corporation, C=US>

<CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US>

<OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US>

<CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB>

<CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE>

<CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US>

<CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US>

<CN=QuoVadis Root CA 2, O=QuoVadis Limited, C=BM>

<CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE>

<CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3>

<CN=DST Root CA X3, O=Digital Signature Trust Co.>

<CN=GeoTrust Global CA, O=GeoTrust Inc., C=US>

<CN=thawte Primary Root CA - G3, OU="(c) 2008 thawte, Inc. - For authorized use only", OU=Certification Services Division, O="thawte, Inc.", C=US>

<CN=EBS-WIN-0SNCU0GA0AM-CA, DC=EBS, DC=QA>

<CN=AGLC5-INCHN-AGLCQA01-CA, DC=AGLC5, DC=SG>

<CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US>

<OID.2.5.4.13=2801931546EP@websense.com, CN=Websense Public Primary Certificate Authority, EMAILADDRESS=support@websense.com, OU=Websense Endpoint, O="Websense, Inc.", L=LG, ST=CA, C=US>

<CN=Microsoft Root Certificate Authority 2011, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US>

<CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright (c) 1997 Microsoft Corp.>

<CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com>

<CN=Development CA>

\*\*\* ServerHelloDone

Warning: no suitable certificate found - continuing without client authentication

\*\*\* Certificate chain

<Empty>

\*\*\*

\*\*\* ClientKeyExchange, RSA PreMasterSecret, TLSv1.2

main, WRITE: TLSv1.2 Handshake, length = 320

SESSION KEYGEN:

PreMaster Secret:

0000: 03 03 53 83 5B A0 2E 69 DF 05 9E 48 C4 54 F4 95 ..S.[..i...H.T..

0010: 04 33 D3 FD 61 7F DB B3 E4 D6 0C B6 4B 30 A9 D9 .3..a.......K0..

0020: B1 CE 26 FD 78 37 BB 14 DC 30 15 32 81 5A F2 91 ..&.x7...0.2.Z..

CONNECTION KEYGEN:

Client Nonce:

0000: 59 F1 D7 97 84 FB 03 48 D0 6B A3 23 31 8E 0B 16 Y......H.k.#1...

0010: 72 BB 1D E8 D7 6A 0A 32 40 DA 11 75 D2 62 1B F0 r....j.2@..u.b..

Server Nonce:

0000: 59 F1 D7 97 89 02 7D 31 C6 DB 81 8F 2E CA B0 EA Y......1........

0010: 7A 3E 0C CB F5 62 02 C5 F5 16 FA E0 7F 77 A7 6B z>...b.......w.k

Master Secret:

0000: A4 45 C1 5C E5 58 11 76 32 1D D1 FB 56 C1 50 A3 .E.\.X.v2...V.P.

0010: 51 92 DF BC A5 BD 5C D7 B3 CA 62 18 2E 09 5A 3C Q.....\...b...Z<

0020: C5 09 A1 AB 0C 5E DD FF 25 A8 5A D1 22 04 8C E1 .....^..%.Z."...

Client MAC write Secret:

0000: E8 80 36 44 E8 99 3F 91 B0 EA 42 4E DF 1B 41 4E ..6D..?...BN..AN

0010: 2B CC D0 9F B9 37 C9 61 11 F3 7C 46 30 71 04 88 +....7.a...F0q..

Server MAC write Secret:

0000: FF 89 B5 28 FB C7 1E A2 EF C3 D3 3B B0 C1 6F 9D ...(.......;..o.

0010: 6F 0C 44 B2 72 E0 1D 98 46 CD C4 97 28 DA 88 50 o.D.r...F...(..P

Client write key:

0000: FB D6 B9 46 DF 25 D9 F3 58 79 D0 F7 CB 2E 11 DD ...F.%..Xy......

Server write key:

0000: 6D 9B 23 8D FF 38 15 07 9B 75 D3 87 43 CB 24 B5 m.#..8...u..C.$.

... no IV derived for this protocol

main, WRITE: TLSv1.2 Change Cipher Spec, length = 64

\*\*\* Finished

verify\_data: { 6, 27, 174, 251, 169, 30, 136, 101, 92, 49, 150, 22 }

\*\*\*

main, WRITE: TLSv1.2 Handshake, length = 80

main, READ: TLSv1.2 Change Cipher Spec, length = 64

main, READ: TLSv1.2 Handshake, length = 80

\*\*\* Finished

verify\_data: { 214, 5, 104, 88, 217, 41, 126, 234, 240, 122, 97, 164 }

\*\*\*

%% Cached client session: [Session-2, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256]

main, READ: TLSv1.2 Application Data, length = 1584

Output from Server ....

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>

<title>403 - Forbidden: Access is denied.</title>

<style type="text/css">

<!--

body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}

fieldset{padding:0 15px 10px 15px;}

h1{font-size:2.4em;margin:0;color:#FFF;}

h2{font-size:1.7em;margin:0;color:#CC0000;}

h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}

#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;

background-color:#555555;}

#content{margin:0 0 0 2%;position:relative;}

.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}

-->

</style>

</head>

<body>

<div id="header"><h1>Server Error</h1></div>

<div id="content">

<div class="content-container"><fieldset>

<h2>403 - Forbidden: Access is denied.</h2>

<h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>

</fieldset></div>

</div>

</body>

</html>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>403 - Forbidden: Access is denied.</title><style type="text/css"><!--body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body><div id="header"><h1>Server Error</h1></div><div id="content"> <div class="content-container"><fieldset> <h2>403 - Forbidden: Access is denied.</h2> <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3> </fieldset></div></div></body></html>

We are struggling with this issue more than a month, It will be great help if someone help us.