Error n°1 : Error while parsing CRL

The “Content-Type” in response is already set to 'application/pkix-crl' as you can see below:

```
mehrez@GOTOUS:~$ wget -c http://crl.certification.tn/TunRootCA2.crl
--2016-01-19 16:18:41--  http://crl.certification.tn/TunRootCA2.crl
Résolution de crl.certification.tn (crl.certification.tn)… 10.10.1.4
Connexion à crl.certification.tn (crl.certification.tn)|10.10.1.4|:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 762 [application/pkix-crl]
Enregistre : «TunRootCA2.crl»

100%[======================================>] 762         --.-K/s   ds 0s

2016-01-19 16:18:41 (109 MB/s) - «TunRootCA2.crl» enregistré [762/762]
```

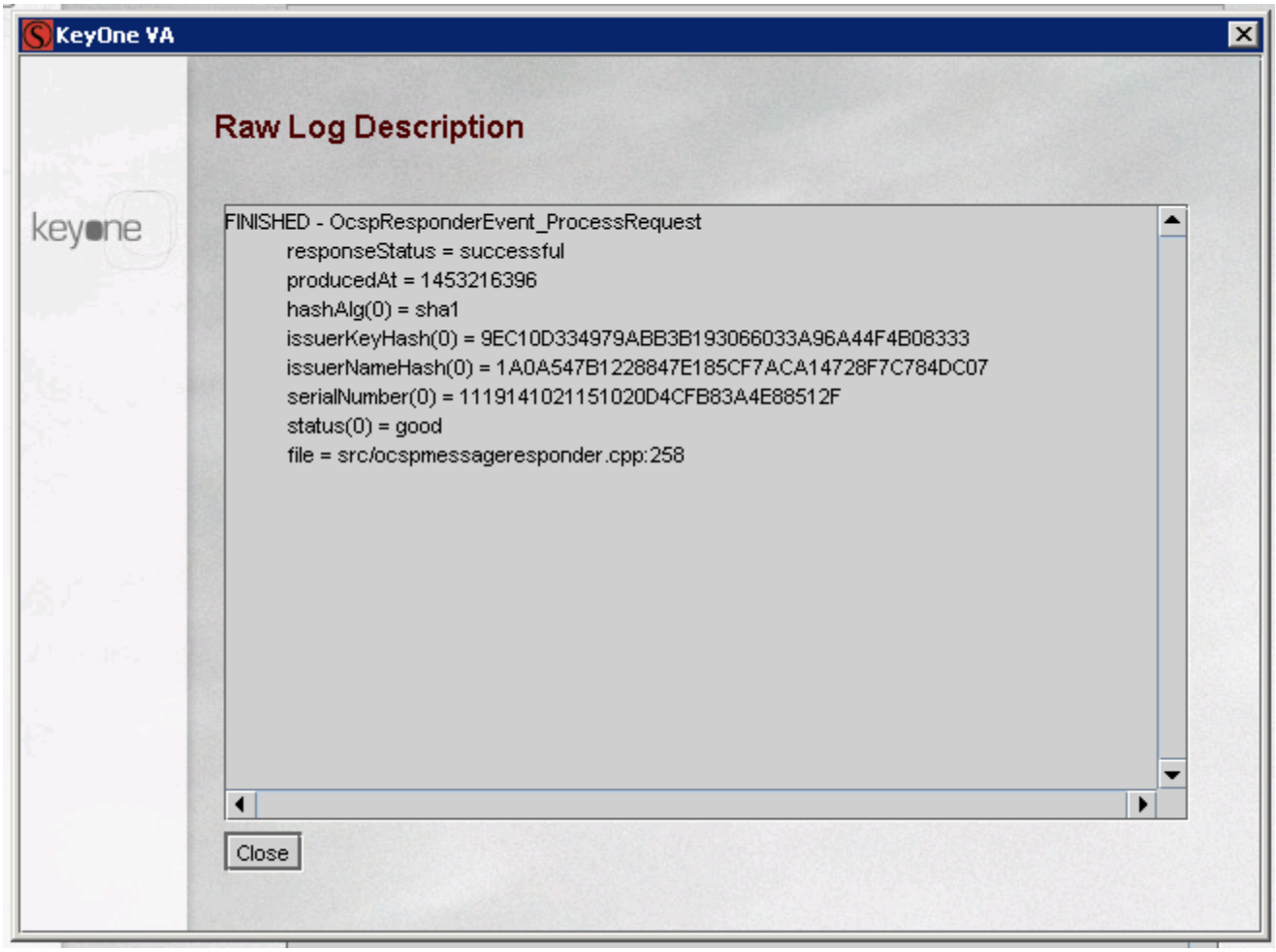
```
mehrez@GOTOUS:~$ wget -c http://crl.certification.tn/TunServerCA2.crl
--2016-01-19 16:18:45--  http://crl.certification.tn/TunServerCA2.crl
Résolution de crl.certification.tn (crl.certification.tn)… 10.10.1.4
Connexion à crl.certification.tn (crl.certification.tn)|10.10.1.4|:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 1295 (1,3K) [application/pkix-crl]
Enregistre : «TunServerCA2.crl»

100%[======================================>] 1 295       --.-K/s   ds 0s

2016-01-19 16:18:45 (133 MB/s) - «TunServerCA2.crl» enregistré [1295/1295]
```

Error N°2 : Error parsing OCSP response: asn1: structure error: tags don't match (16 vs {class:0 tag:28 length:72 isCompound:true}) {optional:false explicit:false application:false defaultValue:<nil> tag:<nil> stringType:0 timeType:0 set:false omitEmpty:false} responseASN1 @2

This problem it's not an OCSP Server problem. As you can see, POST request are resolved correctly.

```
OpenSSL> ocsp -issuer tunserverca2.pem -CAfile tunrootca2.pem -url http://ocsp.c
ertification.tn -cert webmail.crt.cer -VAfile ocsp-2015.crt
Response verify OK
webmail.crt.cer: good
        This Update: Jan 19 12:31:01 2016 GMT
        Next Update: Jan 25 12:31:01 2016 GMT
OpenSSL>
```

The parsing error occurs because when treating the wrong GET request our OCSP Server sends a redirect to a welcome page “ - Welcome to KeyOne VA –“, which logically cause the OCSP response parsing error.



Error N°3: Bad signature on embedded certificate: Authority Key Identifier of Signing certificate (ocsp.certification.tn) is not from Issuer ('Tunisian Root Certificate Authority - TunRootCA2')

The certificate of OCSP contains the Authority Key Identifier below:

keyid:87:AB:F7:69:4B:50:F6:61:57:FF:3F:5B:8E:1D:70:C6:A2:6C:AA:C6

This key id corresponds to the subject key identifier of the TunServerCA2 which is the issuer and not TunRootCA2. You can find the OCSP certificate in attachment.

Error N°4: OCSP signing certificate expires before NextUpdate

This error has already been resolved in the first “OCSP response information “ as you can see below:

Source: Authority Information Access in Certificate
Location: http://ocsp.certification.tn (POST)
Size: 3972 bytes (DER data)
Response time: 660.768466ms
Signature algorithm: SHA256WithRSA
Signature type: CA Deligated
Signed by: ocsp.certification.tn
Issued by: Tunisian Server Certificate Authority - TunServerCA2
Reported statuses: 1
This update: Wednesday, 13 January 2016 12:30 UTC
Next update: Tuesday, 19 January 2016 12:30 UTC
Produced at: Wednesday, 13 January 2016 21:18 UTC
Status: Good

Relevant server response headers

Date: Wednesday, 13 January 2016 21:18 UTC
Expires: Thursday, 1 January 1970 00:00 UTC

✔ OCSP signing certificate is already valid
✔ OCSP signing certificate is not expired
✔ OCSP signing certificate does not expire before NextUpdate
✔ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing