2 Проблемы с сертификатами

OpenSSL используется с CRL и по некоторым CA в цепочке сертификатов их CRL не включены в ''TLSCRLFile''

В журнале TLS сервера в случае *mbed TLS (PolarSSL)* и *OpenSSL* узлов:

```
failed to accept an incoming connection: from 127.0.0.1: TLS handshake with
127.0.0.1 returned error code 1: \
    file s3_srvr.c line 3251: error:14089086: SSL
routines:ssl3_get_client_certificate:certificate verify failed: \
    TLS write fatal alert "unknown CA"
```

В журнале TLS сервера в случае *GnuTLS* узла:

```
failed to accept an incoming connection: from 127.0.0.1: TLS handshake with
127.0.0.1 returned error code 1: \
    file rsa_pk1.c line 103: error:0407006A: rsa
routines:RSA_padding_check_PKCS1_type_1:\
    block type is not 01 file rsa_eay.c line 705: error:04067072: rsa
routines:RSA_EAY_PUBLIC_DECRYPT:paddin
```

CRL устарел или срок действия истечет в процессе операции сервера

OpenSSL, в журнале сервера:

- до истечения срока действия:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot
establish TLS to [[127.0.0.1]:20004]:\
    SSL_connect() returned SSL_ERROR_SSL: file s3_clnt.c line 1253:
error:14090086:\
    SSL routines:ssl3_get_server_certificate:certificate verify failed:\
    TLS write fatal alert "certificate revoked"
```

- после истечения срока действия:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot
establish TLS to [[127.0.0.1]:20004]:\
    SSL_connect() returned SSL_ERROR_SSL: file s3_clnt.c line 1253:
error:14090086:\
    SSL routines:ssl3_get_server_certificate:certificate verify failed:\
    TLS write fatal alert "certificate expired"
```

Дело в том, что при наличии действительного CRL аннулированный сертификат записывается как “certificate revoked”. При истекшем CRL сообщение об ошибке меняется на “certificate expired”, которое может ввести в заблуждение.

GnuTLS, в журнале сервера:

- до и после истечения срока действия одинаково:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot
establish TLS to [[127.0.0.1]:20004]:\
      invalid peer certificate: The certificate is NOT trusted. The
certificate chain is revoked.
```

mbed TLS (*PolarSSL*), в журнале сервера:

- до истечения срока действия:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot
establish TLS to [[127.0.0.1]:20004]:\
    invalid peer certificate: revoked
```

- после истечения срока действия:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot
establish TLS to [[127.0.0.1]:20004]:\
      invalid peer certificate: revoked, CRL expired
```