Online Certificate Status Protocol (OCSP)
On-line revocation/status checking availability

EKENG provides real-time certificate status verification service OCSP – according to RFC 2560. Using OCSP, it is possible to acquire more frequent and up-to-date information (in comparison to CRL usage) about a certificate status. Public interface based on Online Certificate Status Protocol responding for certificate validity requests. OSCP Responder relies on its database resource updated on demand by CA module after certificate status change.
OCSP supplies the following information about the certificate status:

Good – meaning a positive response to the request, which should be interpreted as confirmation of certificate validity,
Revoked – meaning the certificate has been revoked,
Unknown – meaning the certificate has not been issued by any of the affiliated certification authorities.

Example:

ocsp -CAfile [CA Certificate Name] -issuer [Issuer Certificate] -url http://ocsp.pki.am/ocsp -serial [certificate serial number]

Access to service will be available only after validation and signing of contract with EKENG CJSC