OCSP for IGTF CAs

Milan Sova

Requirements

- preferably light-weight service (RFC5019)
  - pre-generated responses
    (signed by the issuing CA's key)
  - HTTP GET
    (caching)

Software by CESNET PKI

- PHP+Apache
  - PKIMessage library
- usable for
  - RFC 5019-compliant OCSP server (pre-generated responses)
  - forwarding OCSP server (eg. GET to POST)
- to be released for EUGridPMA meeting in Lyon (Sep 2012)

To solve

- by IGTF
  - validity period of responses
  - same as current CRLs?
- by CAs
  - pre-generation of responses