OCSP Algorithm Agility

Problem 1: No guidance

- OCSP says nothing about selecting the signing algorithm
  - It probably should
  - Alternative is to guess
  - Guesses lead to interoperability failure

Problem 2: May require different algorithm

- Large infrastructures require independent components
  - OCSP signer separate from cert signer
  - OCSP verification separate from relying app.
  - May be separately validated
  - Algorithm selection heuristics will fail
    - OCSP responder does not know the certificate alg.
    - Neither does the verifier!

Solution

1. Document selection process to be used
2. Allow client to tell server what they want