OCSP Algorithm Agility

Problem

- RFC 2550 does not specify how the responder chooses the signature algorithm
  - This was not a problem when RSA-SHA1 was only signature required
    - RSA-SHA256 created issues
    - More issues will be raised with ECC transition
  - This should be fixed
    - Fix should be same standards status as OCSP

The Reasonable Assumption

- OCSP responder signs response with same signature type as the certificate being queried

- Problems
  - What if there is no match for the cert?
  - What if the signer does not have a signing cert for the certificate algorithm?
  - What if the verifier does not have ability to verify the certificate algorithm?

The Comprehensive Solution

- Requestor may specify supported algorithms
    - Simple OCSP extension
- If no algorithm specified default to:
    - Certificate signature algorithm (if known)
    - Default policy (if configured)
    - RSA-256

Proposal

- PHB submits new ID to clarify this case
  - Standards track

- Merge into base OCSP spec if general revision takes place.