OCSP Response Extension

Rich Salz

Goal

- Given increased use of OCSP stapling, allow a “hint” to be given to the operator when their TLS server cert is revoked
- Server can query its status; if the response is revoked, display the value of the extension
  - “The check bounced”
  - “Revoked by ticket #123123 opened by rsalz”

ASN.1

```
id-pkix-ocsp-revoke-hint OBJECT IDENTIFIER
      ::= { id-pkix-ocsp TBD }

re-ocsp-revoke-hint EXTENSION {
     SYNTAX UTF8String
     IDENTIFIED BY id-pkix-ocsp-revoke-hint
}
```

Implementation

- OpenSSL next release would have it
- CA/B Forum will probably eventually profile against it