Multiple OCSP Responses

In TLS Handshake

draft-pettersen-tls-ext-multiple-ocsp-03

Yngve N. Pettersen

Opera Software ASA

Problem statement

- Using TLS OCSP Stapling for intermediate CA certificates would give more timely revocation information to clients
- Will improve user experience, lower workload for CAs, slightly increase bandwidth usage for sites
- The current status_request extension only allows OCSP for the site certificate, and adding more methods is not feasible due to design limitations
- A new extension that allows multiple status methods is needed

Current status of -03

- Implementation revealed a design problem with future addition of new status request methods
- Older implementations would not be able to read the new status request records
- Fixed this problem by adding a length field for the request field in status request records
- The same design problem was found to affect two existing extensions: SNI and Trusted CA

Way forward

- The document is based on an existing extension
- The document is near technical completion
- Request that draft be handled as TLS WG item since it replaces an existing RFC 6066 extension

Appendix: The variant record issue

Client

```
enum{
  Foo, Bar, Wha1;
} Typ

struct {
  Typ rec_typ;
  Select(rec_typ)
  {
    case Foo: opaque food<1..2^8-1>;
    case Bar: opaque barge<1..2^16-1>;
    case Wha1:
       opaque whatsths<1..2^8-1>;
       opaque whatstht<1..2^16-1>;
  } payload;
}Rec;

Rec Recs<1..2^16-1>;
```

Server

```
enum{
  Foo, Bar;
} Typ

struct {
  Typ rec_typ;
  Select(rec_typ)
  {
    case Foo: opaque food<1..2^8-1>;
    case Bar: opaque barge<1..2^16-1>;
  } payload;
}Rec;

Rec Recs<1..2^16-1>;
```

Appendix: The variant record issue

Client	Server
vector length	OK
Bar	OK
Payload.barge ABCDEF	OK Payload.barge ABCDEF
Wha1	??? Unknown type. Will ignore following content.
Payload.whatsths HJKLMN	Huh? What's this? Don't know how to parse it. Exception!
Payload.whatstht OPQRS	Exception!
Foo	Exception!
Payload.food TUVWXYZ	Exception!

Appendix: The variant record issue

Client

```
enum{
  Foo, Bar, Wha1;
} Typ

struct {
  Typ rec_typ;
  uint16 payload_length;
  Select(rec_typ)
  {
    case Foo: opaque food<1..2^8-1>;
    case Bar: opaque barge<1..2^16-1>;
    case Wha1:
       opaque whatsths<1..2^8-1>;
       opaque whatstht<1..2^16-1>;
  } payload;
}Rec;

Rec Recs<1..2^16-1>;
```

Server

```
enum{
  Foo, Bar;
} Typ

struct {
  Typ rec_typ;
  uint16 payload_length;
  Select(rec_typ)
  {
    case Foo: opaque food<1..2^8-1>;
    case Bar: opaque barge<1..2^16-1>;
  } payload;
}Rec;

Rec Recs<1..2^16-1>;
```

Appendix: The variant record issue

Client	Server
vector length	OK
Bar	OK
length of Payload	OK
Payload.barge ABCDEF	OK Payload.barge ABCDEF
Wha1	??? Unknown type. Will ignore following content.
length of Payload	OK
Payload.whatsths HJKLMN	Ignoring this, since I don't know what it is
Payload.whatstht OPQRS	Ignoring this, since I don't know what it is
Foo	OK
length of Payload	OK
Payload.food TUVWXYZ	OK Payload.food TUVWXYZ