Additional PRF input draft-solinas-tls-additional-prf-input

Hiroshima, November 2009

Paul Hoffman, VPN Consortium

Purpose

- Some people want additional data to be included in the master secret calculation (inside the PRF, of course)
- Give a single generic structure for adding this instead of requiring each extension to define how its material would get mixed into the PRF

Mechanism

```
struct {
   uint16 AdditionalPRFInputType;
   opaque AdditionalPRFInputValue<0..2^16-4>;
} AdditionalPRFItem;
struct {
  AdditionalPRFItem item_list<0..2^16>
} AdditionalPRFInput;
```

- IANA registry for types
- Two types defined
  - Additional random (any size)
  - OtherInfo for NIST SP 800-56A

Status

- Simon pointed out in the -00 that there was no structure, so it was added
- Pasi pointed out in the -01 that this new extension allows TLS extensions without IETF consensus
  - Have some possible ways forwards to prevent this hole
- No other issues so far