Recent IKEv2bis activity

Paul Hoffman

IPsecME WG virtual interim, 2009-09-22

#22 - Add section on simultaneous IKE SA rekey
Tero suggests that we copy the material from the IKEv2 Clarifications document; Yaron agrees. Paul doesn't like this unless some implementers read it carefully again.

#26 - Missing treatment of error cases
Edited Tero's most recent wording and inserted it in the next draft. Already received some comments on the list; would like to have more.

#28 - Obtaining src/dest IP addresses for UDP-encapsulated transport mode ESP
Added Tero's text as section 2.23.1. Removed any mention of RFC 3947, which is not part of IKEv2. Already received some comments on the list; would like to have more.

#79 - Remove CP from Create_Child_SA?
There was no agreement on this. We should probably close out the issue unless those interested can agree on the semantics.

#107 - Sending certificate chains in IKEv2
Added "Note that with this encoding, if a chain of certificates needs to be sent, multiple CERT payloads are used, only the first of which holds the public key used to validate the sender's AUTH payload." But there may be more to say...

Next up - Issue the -05 draft
Will probably have it ready to submit in about two weeks. Will maybe close out some easy open issues before then.