Minimal IKEv2

AuthenTec Oy
Tero Kivinen
kivinen@iki.fi
draft-kivinen-ipsecme-minimal-ikev2-01

What Problem Does This Document Solve

- Tries to educate implementors that IKEv2 is not complex and difficult to implement.

Why Do People Consider IKEv2 Complex

- IKEv2 looks quite complicated because there is so many optional features
  - Optional things include:
    - Working as responder, SA management, rekeying, NAT-T, Configuration payloads, EAP authentication, Cookies, Multiple child SAs
- IKEv2 can be implemented without any of those optional features, and then it comes quite small and simple.

Implementation Experience

- There is 2 minimal implementations of IKEv2 both less than 1000 lines of source code (perl and python).
  - Our full IKEv2 library is 44k lines of C
  - Cert library is 56k lines, or 81k lines of enrollment and CRL retrieval is included
- Implementing minimal IKEv2 is very simple compared to full implemention.
- There are some optimizations which can be done when only supporting minimal set of features.

Summary

- This document does not change anything in the RFC5996.
  - Except it profiles X.509 certificate authentication out
- Explains the mandatory minimal features, leaving out all the optional things to make it short and simple.