Requirements for IPsec Negotiation in the SIP Framework

draft-saito-mmusic-ipsec-negotiation-req-02.txt

March 20, 2006

Makoto Saito (ma.saito@nttv6.jp)
Shingo Fujimoto (shingo_fujimoto@jp.fujitsu.com)

Motivation

- Using IPsec for the Media Security
- Use Cases of IPsec
  - Vendor proprietary protocol.
  - Aggregation of a large number of media.
  - L2TP with IPsec may be used to encrypt media.

IPsec is a simple and comprehensive way
in these cases.

Key-Exchange Methods

- IKE - Standard One
- Sdescriptions and Key-mgmt

  "Advantages of Using SDP"

  – Simple round-trip

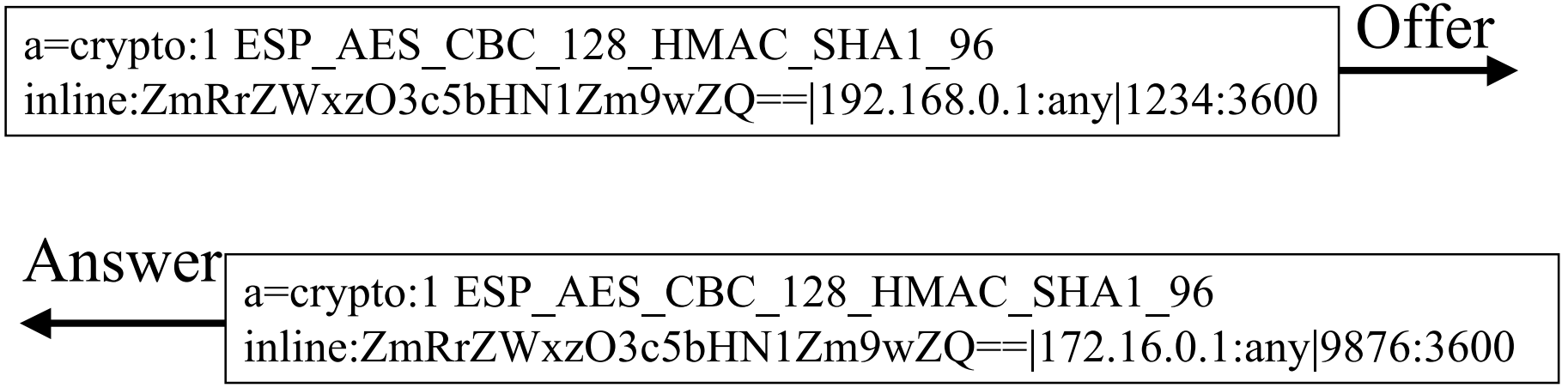
  – Synchronization with the state of media session (start, refresh, end)

One of Proposals

Using Sdescriptions

- General framework
- Only a profile of SRTP is defined for now
- Just adding a profile for IPsec (SA proposal) here

  Ex: key material, IP address, spi, life time, etc.



Next Step

- Thinking of detailed technical spec.
- Any Comments?
- Interest?