



IP address update

NOTIFY_UPDATE: ESP_INFO,
ECHO_REQUEST_SIGNED, HMAC, sig

NOTIFY_UPDATE_ACK: ACK,
ECHO_RESPONSE_SIGNED, HMAC, sig

UPDATE: ESP_INFO, HMAC_ESP_INFO,
LOCATOR, SEQ, HMAC.MR, sig

UPDATE: ESP_INFO, HMAC_ESP_INFO, LOCATOR,
SEQ, ACK, ECHO_REQUEST, HMAC, sig

UPDATE: ACK, ECHO_RESPONSE,
HMAC.MR, sig

IPsec ESP protected data

- Check signature
- Check HMAC
- Store new INDEX
- Generate new keys

- Check signature
- Check HMAC

- Check signature
- Check HMAC
- Store new IP.MR
- Store new INDEX
- Generate new keys