ESP transform in HIP draft-jokela-hip-esp-00

Petri Jokela and Pekka Nikander
HIP working group
62nd IETF, Minneapolis

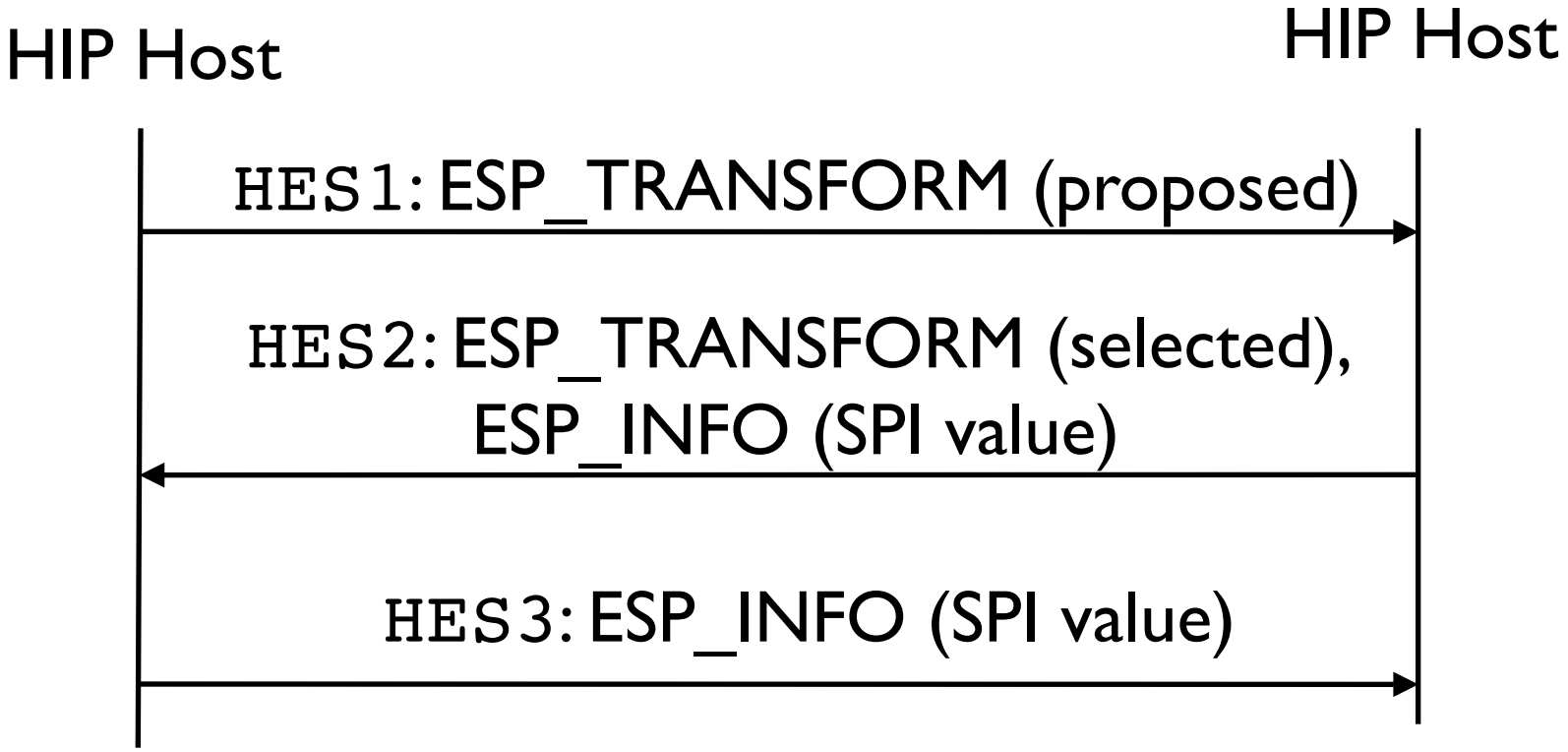
Purpose of this draft

- Defines the ESP transform usage with HIP
  - Originally included in HIP base spec -01
  - Mandatory for HIP implementations
- Functionality
  - Setting up ESP SAs between HIP nodes
  - Updating an existing ESP association (rekeying)

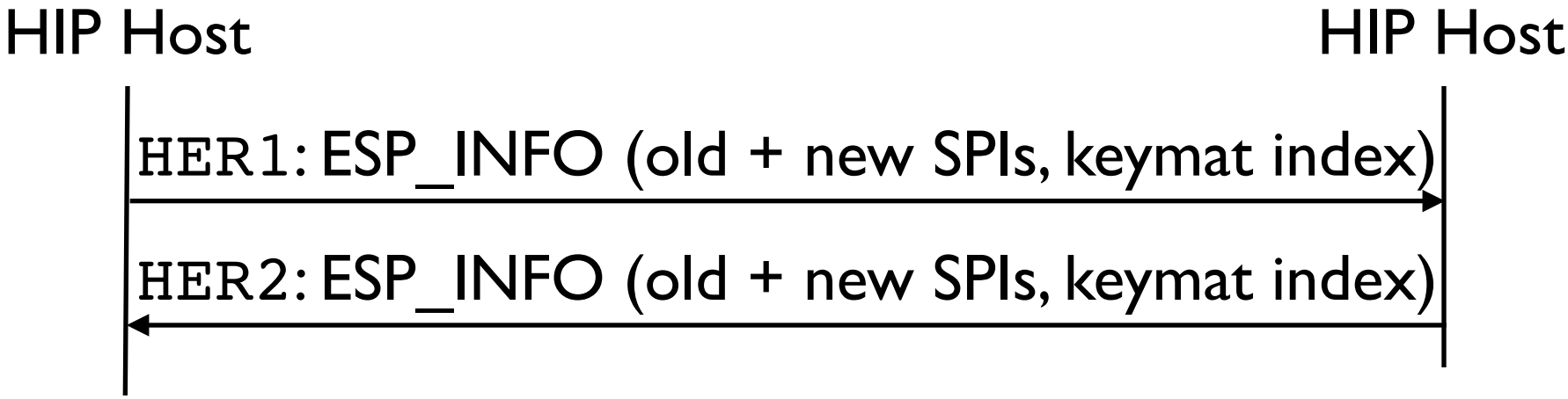
Parameters

- ESP_INFO
  - Combines earlier SPI and NES parameters
  - Remote's old SPI, new SPI, KEYMAT index
- ESP_TRANSFORM
  - Encryption and authentication transforms
- New NOTIFY error types
  - NO_ESP_PROPOSAL_CHOSEN
  - INVALID_ESP_PROPOSAL_CHOSEN

Setting up a new ESP SA pair



Updating an existing ESP SA pair



Open issues

- Shall we maintain the current ”look”
  - Conceptual packet exchanges (HER, HES)

    or
  - Parameters tightly bound to the base exchange and UPDATE packets as it was in base draft -01
- ESP support a MUST implement protocol
- Sections 3 and 4 will be re-written

Next steps

- Adopt as a working group draft?
- Issue a revised version in April
- Proceed hand-in-hand with the base spec