# Responder Initiated Address Update in MOBIKE

**draft-smyslov-ipsecme-ikev2-r-mobike**

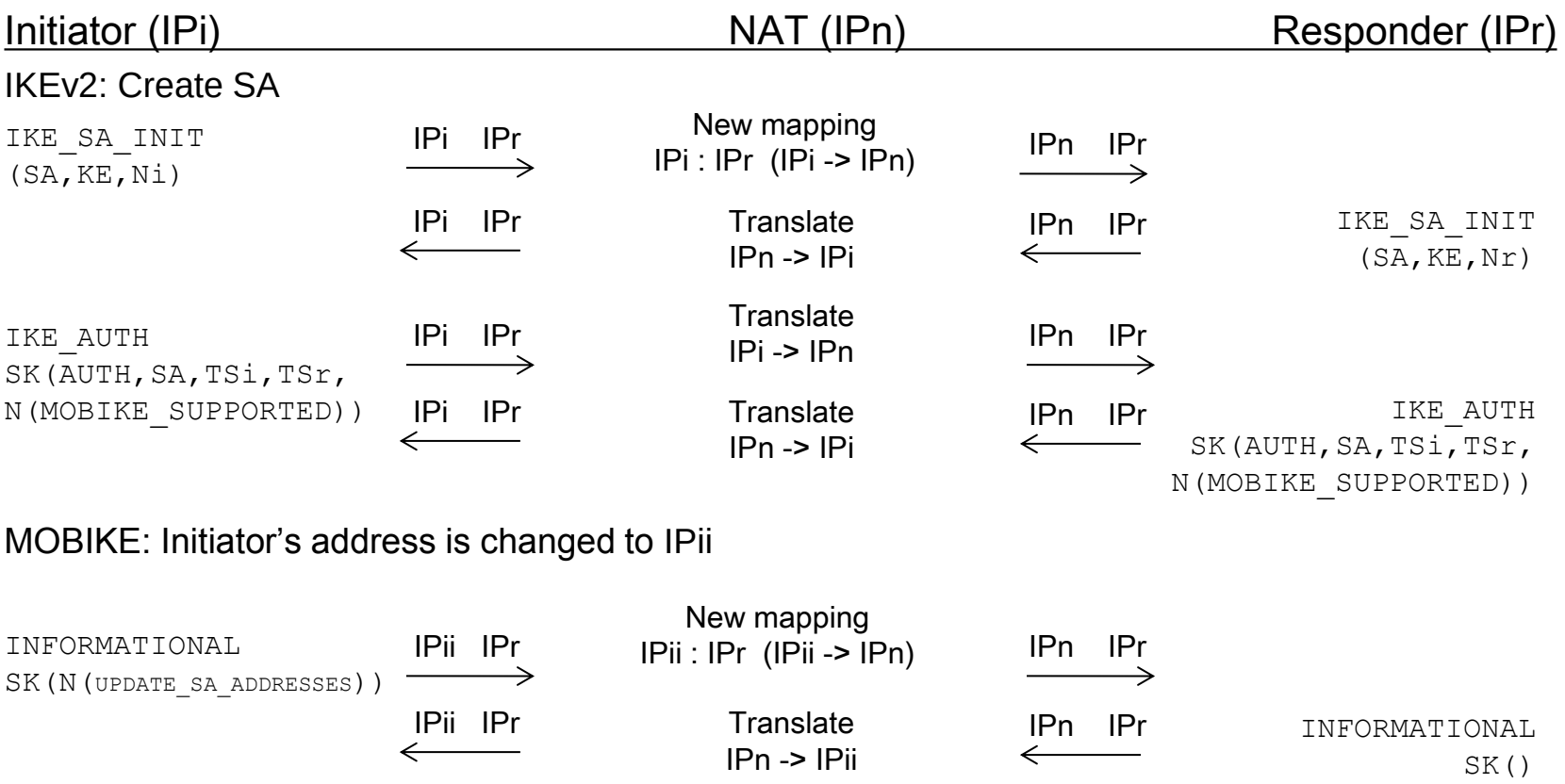
Valery Smyslov
svan@elvis.ru

IETF 99

# MOBIKE

- MOBIKE (IKEv2 Mobility and Multihoming Protocol, RFC4555) allows peers to change their IP addresses without re-establishing existing SAs
- To change IP address of an SA the original IKEv2 Initiator initiates `INFORMATIONAL` exchange containing `UPDATE_SA_ADDRESSES` Notification, using new IP address

# MOBIKE Operations



# MOBIKE Limitation

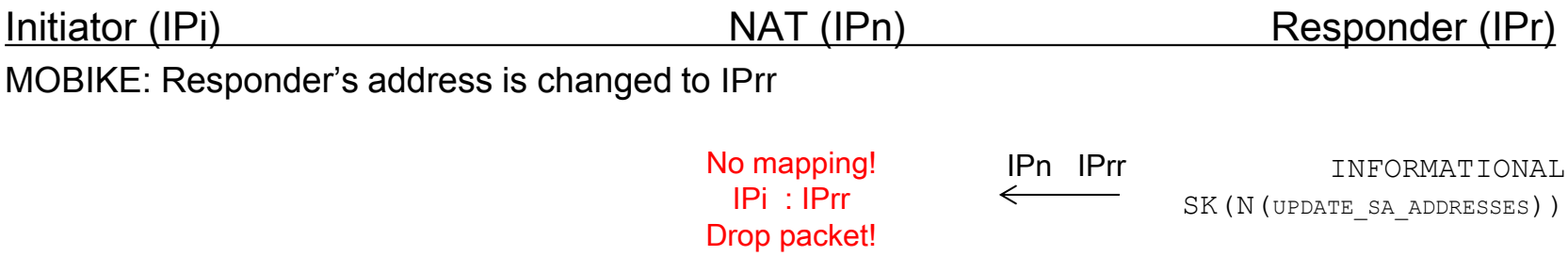
It is original Initiator who is responsible for initiating IP address update, original Responder mostly plays passive role (Section 2.1 of RFC4555).

If NATs are present, then depending on NAT behavior:

- original Responder may not be able to initiate update procedure in case its address changes
- if original Responder is multihomed, it may not be able to instruct original Initiator to switch SAs to another address
  - MOBIKE permits original Responder to try address update procedure in some situations, but in presence of NATs it will probably fail
  - MOBIKE has a “NAT Prohibition” mode, in which SA fails if NAT is detected, however this mode in not useful, since nowadays NATs are almost everywhere

# Cause of the Limitation

- Network asymmetry introduced by “restricted cone” NATs




Result: exchange failed, SA deleted

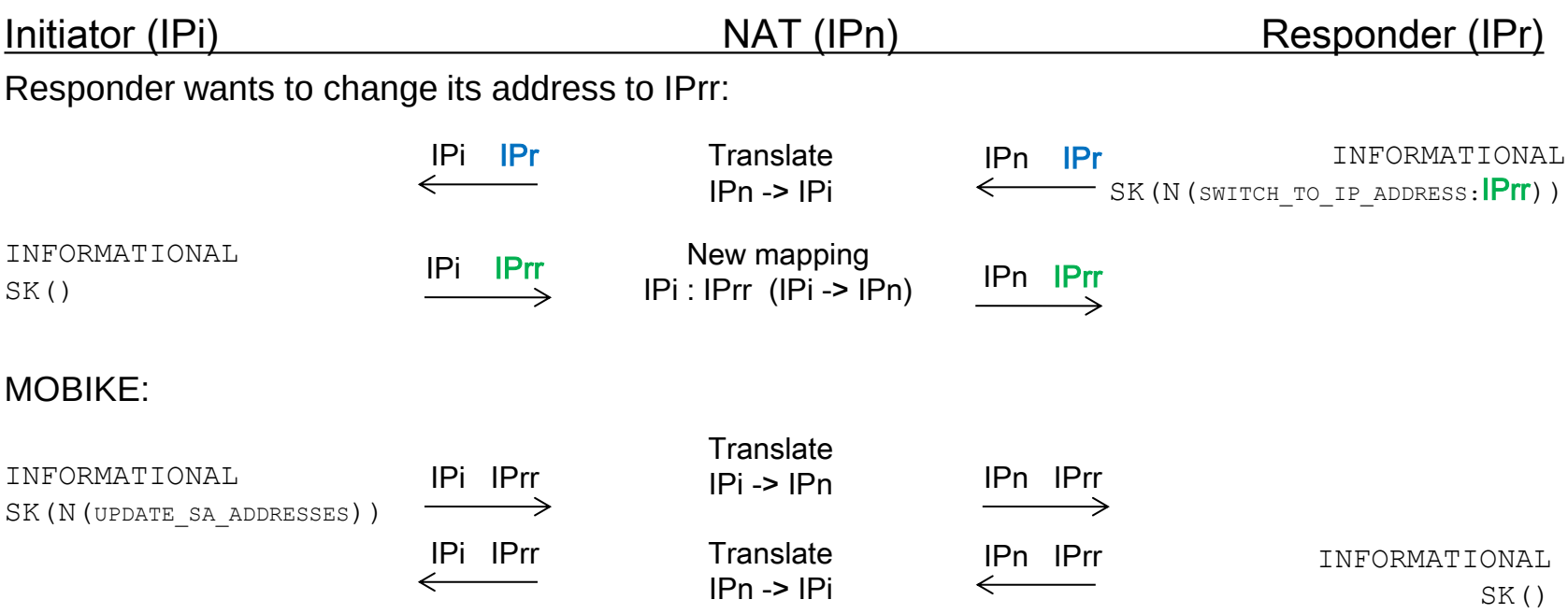
# Negative Effect of the Limitation

- If Responder is a cluster, comprising of nodes each having its own IP address, but sharing security credentials, then SAs, once established with one of the nodes, cannot be moved to another node on cluster's will (e.g. for load balancing)
  - IKE Redirect can accomplish the task, but it requires SA re-establishing
- If Responder's address is changed, then existing SAs cannot be quickly moved to a new IP address; the Initiator needs to figure out new Responder's address (e.g. via DNS) and re-establish SAs
- If Responder is multihomed and one of its interfaces shuts down, it cannot quickly instruct Initiator to move existing SAs to another address; in general it has to wait until Initiator detects the failure

# Proposed Solution

- Responder requests Initiator to move SA to a new Responder's address by initiating `INFORMATIONAL` exchange containing a new status Notification – `SWITCH_TO_IP_ADDRESS`, which contains new Responder's address
- To deal with middleboxes the request is sent using **old** Responder's address, even if it is already unavailable
- The Initiator responds to the **new** Responder's address (supplied in the notification data), thus creating a new mapping on middleboxes
  - violation of Section 2.11 of RFC7296
- Then Initiator immediately starts standard MOBIKE procedure for updating SA addresses

# The Solution Operations



# Interaction with MOBIKE

- Proposed solution is an extension of MOBIKE
- Initiator indicates support for this extension by sending modified `MOBIKE_SUPPORTED` Notification in `IKE_AUTH` Exchange – the Notification contains some predefined data
- If Responder doesn't support the extension, the extra data will be ignored and the Responder never requests updating IP address
- There is no need to negotiate the extension, it's enough if Initiator indicates support for it

# Thanks

- Comments? Questions?
- More details in the draft
- Please review and send feedback to author
- WG adoption?