SEND WG

Chairs: James Kempf, Pekka Nikander

56th IETF, San Francisco Hilton, Tuesday March 18th, 2003

`http://www.tml.hut.fi/~pnr/SEND/slides.pdf`

Agenda bashing

- 5 min. - Agenda discussion
- 10 min. - Last Call Issues for draft-ietf-send-psreq.txt
- 10 min. - Self Signed Certificates for CGAs
- 20 min. - Open Issues on draft-ietf-send-ipsec-00.txt
- 10 min. - Interaction with PANA / DHCP
- 5 min. - Draft Status and Schedule

- Drafts:
  - draft-ieft-send-psreq-02.txt (to be submitted)
  - draft-ietf-send-ipsec-00.txt
  - draft-aura-cga-00.txt (not a WG item)

draft-ietf-send-psreq.txt

- WG Last Call from Jan 23 until Feb 6.
  - Thanks for everybody who cared to comment!
- 26 issues filed in addition to editorial comments
  `http://www.tml.hut.fi/~pnr/SEND/issues.html`
- 1 issue later *merged* to another (#23 to #2)
- 12 issues resolved by *adding* more explanation
- 1 issue resolved by *removing* confusing text
- 6 issues *adopted* by adding the suggested text
- 4 issues (#2, 9, 21, 24) *rejected*
  - More on these on a separate slide
- 2 issues (#1 and #11) *resolved* after discussion
  - More on these on separate slides

Rejected issues

- 2 Clarify the scope of the work
  - The WG charter is clear enough
  - Did not contain any concrete proposals
- 9 Remove mitigation approaches from 4.3.1
  - Based on resolving issue #1; a separate slide later
- 21 Add a note about DDNS access controls
  - Valid comment but out of scope
- 24 Replace the current 3 trust scenarios
  - Rejected after discussion; working group consensus

Issue #11: Using the term "trust"

- Draft-01 reads: It should be noted that the term "trust" is used here in a rather non-technical *and loose* manner.
- Issue: The whole point of this document is to define trust models, so very rigid uses of to trust, trusted, and trusting are important.
- Further comment: Avoid using the term altogether
- Resolution:
  - Scanned all instances of "trust" etc.
  - Each instance seemed to be qualified
  - Removed the words "and loose" from the text above
- Personal comment: I am not really happy with this resolution, but IMHO it is probably good enough

Issue #1: Solution suggestions

- Draft-01 includes multiple suggestions for possible solutions, with the following disclaimer:
  - [T]he [solution] discussion is solely for illustrative purposes. It is meant to give the readers a more concrete idea of some possible solutions. It does NOT indicate any preference on solutions on the behalf of the authors or the working group.
- Issue: Why there is a need to talk about solutions?
- Opinions on the mailing list were mixed:
  - Some people supported solution examples
  - Others opposed including them to the text
- Currnently there are solution examples, in [[brackets]]
- Question: Should the brackets be removed, or the solution examples be removed?

Self signed certificates for CGA

- draft-aura-cga-00.txt
- A separate set of slides

draft-ietf-send-ipsec-00.txt

- A separate set of slides

Interaction with PANA / DCHP

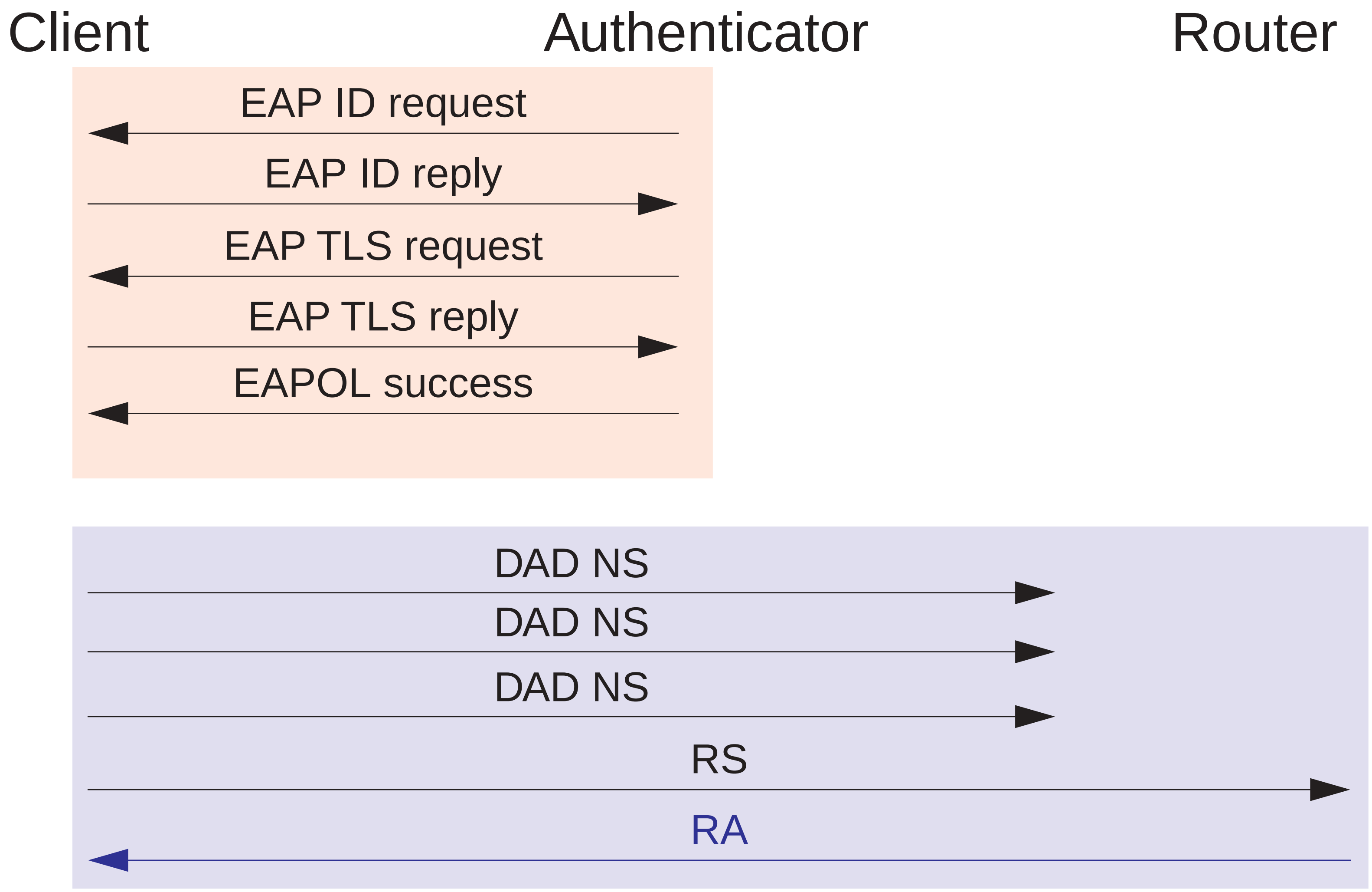
- SEND does not deal with access control
- PANA is mostly about network access control

- SEND only deals with ND, RD, and stateless autoconfig
- DHCP deals with stateful (server provided) autoconfig

- Usage scenarios
  - Baseline: Link layer authentication and SEND
  - SEND and PANA
  - SEND, PANA, and DHCP

Baseline: Link layer auth and SEND

- Client is first authenticated with 802.1x
- Once accepted to the network, required to use SEND



Client

Authenticator

Router

EAP ID request

EAP ID reply

EAP TLS request

EAP TLS reply

EAPOL success

DAD NS

DAD NS

DAD NS

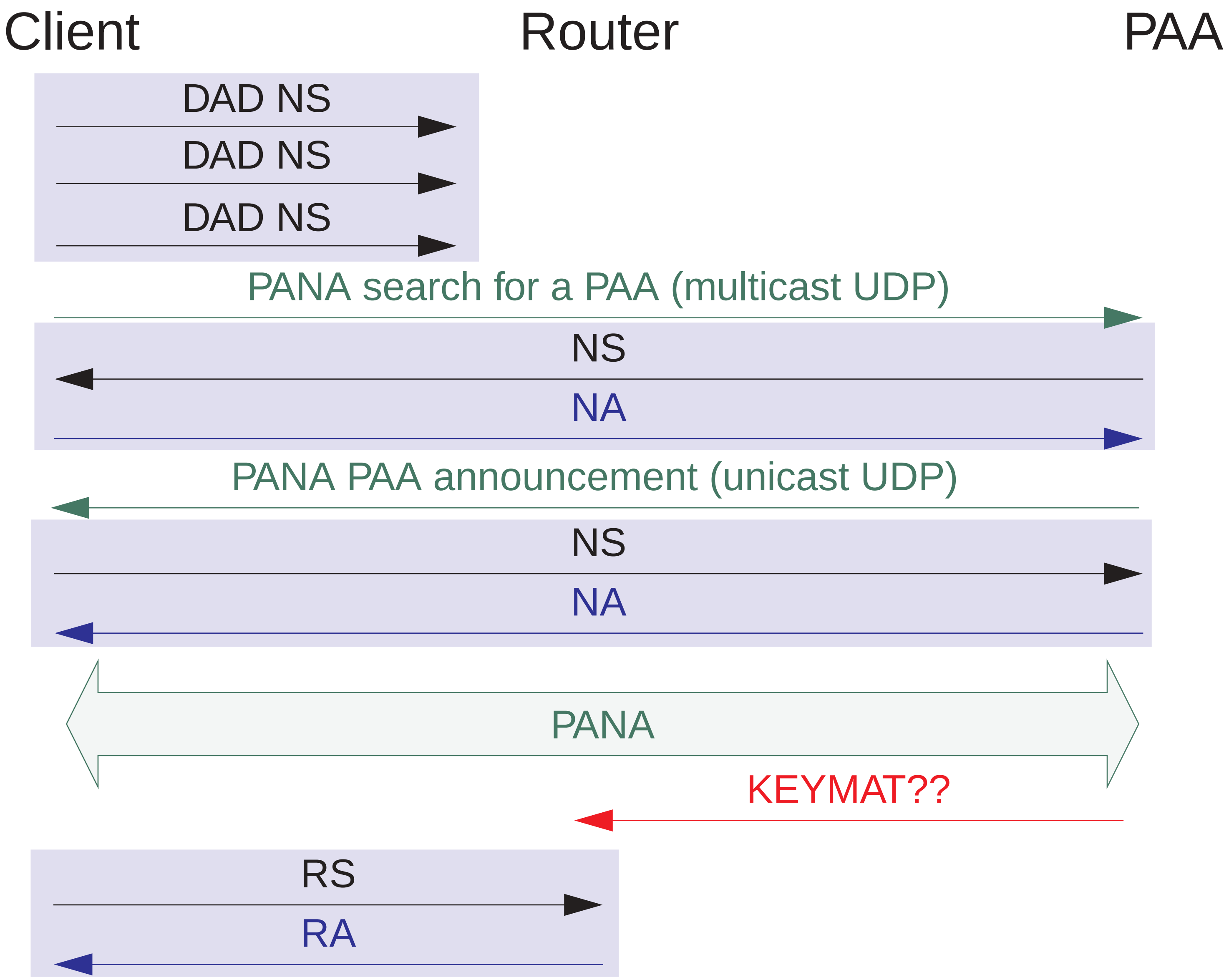
RS

RA

SEND and PANA

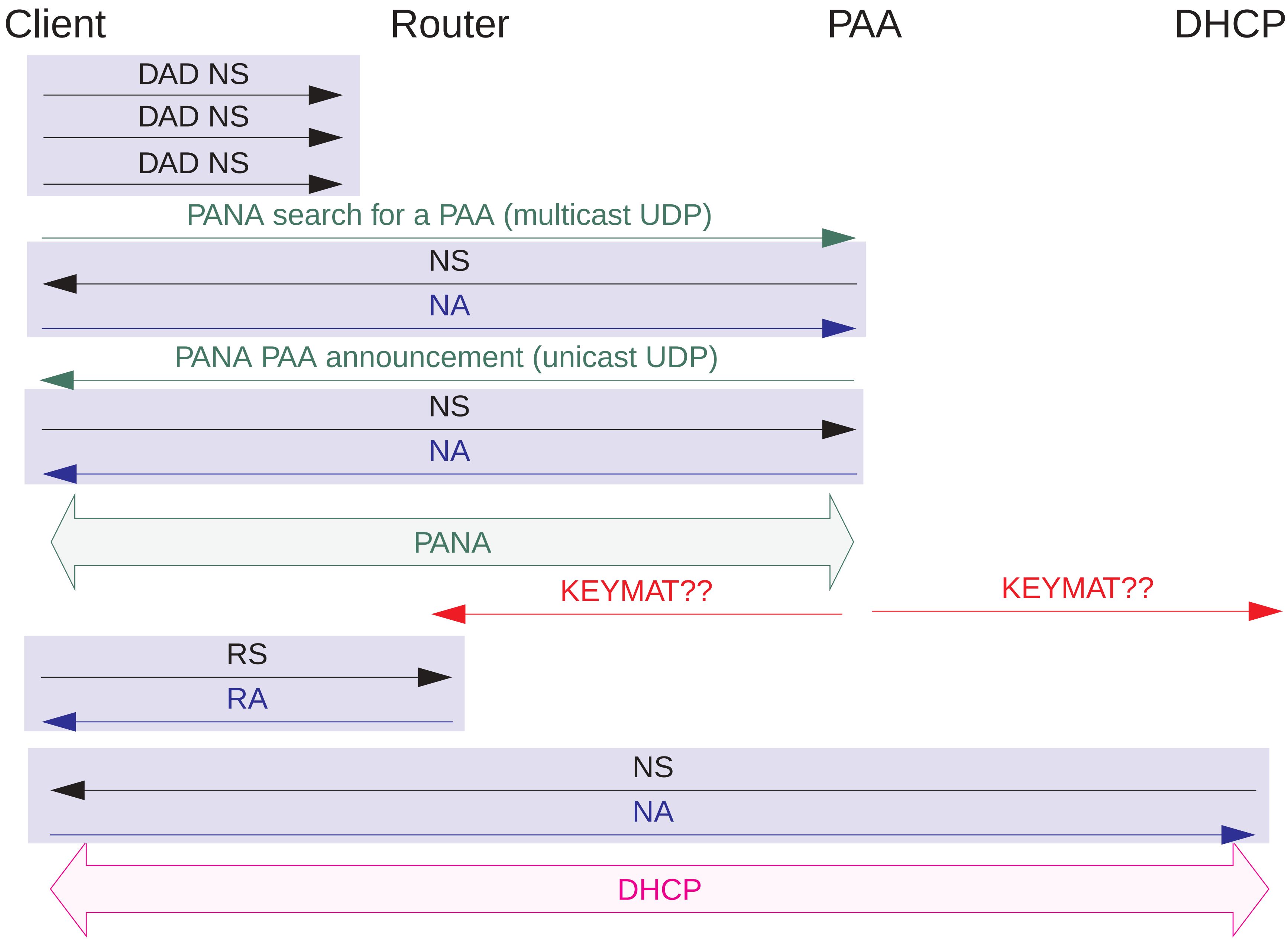
- Client gets a link local address with SEND
- Using the link local address, it searches for a PAA
- PAA performs ND and sends back a reply
- Client performs ND and runs PANA with the PAA
- PANA creates key material
    - Also for Client - Router communication
- Client authenticates RA with the PANA key material

SEND and PANA


Client
Router
PAA
DAD NS
DAD NS
DAD NS
PANA search for a PAA (multicast UDP)
NS
NA
PANA PAA announcement (unicast UDP)
NS
NA
PANA
KEYMAT??
RS
RA

SEND, PANA and DHCP

- Same as SEND and PANA until Router Adverticement
  - Should PANA create keymat also for DHCP?
- Once the client receives RA, it runs DHCP



Client

Router

PAA

DHCP

DAD NS

DAD NS

DAD NS

PANA search for a PAA (multicast UDP)

NS

NA

PANA PAA announcement (unicast UDP)

NS

NA

PANA

KEYMAT??

KEYMAT??

RS

RA

NS

NA

DHCP

Draft status and schedule

- draft-ietf-send-psreq-02.txt to the IESG

- draft-ietf-send-ipsec-00.txt
  - Should we split PK AH into a separate draft?
  - Should we split CGA into a separate draft?
  - Do we need a CGA-free version?
  - How to do Proxy ND?
  - Getting a regression of the protocol against the threats document?

Steps forward

- Run the DT for another couple months to resolve the remaining technical issues
- Continue talking with IPR holders on CGA to get IPR released specifically for SEND
- Generate another draft version (or two) pre-Vienna
- Line up a panel of dedicated reviewers (implementors, security Steves, an OPS person) to do a preIESG review
- If there are no show-stopper technical issues and CGA IPR gets resolved, submit to IESG post-Vienna