Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

• By participating in the IETF, you agree to follow IETF processes and policies.
• If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
• As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
• Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
• As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam ([https://www.ietf.org/contact/ombudsteam/](https://www.ietf.org/contact/ombudsteam/)) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

• BCP 9 (Internet Standards Process)
• BCP 25 (Working Group processes)
• BCP 25 (Anti-Harassment Procedures)
• BCP 54 (Code of Conduct)
• BCP 78 (Copyright)
• BCP 79 (Patents, Participation)
• [https://www.ietf.org/privacy-policy/](https://www.ietf.org/privacy-policy/) (Privacy Policy)
Administrative Tasks

Bluesheets
We need volunteers to be:
• Two note takers
• One jabber scribe

Jabber: xmpp:ipsecme@jabber.ietf.org?join
MeetEcho: http://www.meetecho.com/ietf104/ipsecme/
Etherpad:
https://etherpad.tools.ietf.org/p/notes-ietf-104-ipsecme
Agenda

• Agenda bashing, Logistics – Chairs (5 min) (10:50-10:55)
• Draft Status – Chairs (10 min) (10:55-11:05)

• Work items
  • Intermediate Exchange in the IKEv2 Protocol - Valery Smyslov (10 min) (11:05-11:15)
  • Post-quantum Key Exchanges in IKEv2 - Valery Smyslov (10 min) (11:15-11:25)
  • An implementor's view on Hybrid PQKE in IKEv2 - Tobias Heider (10 min) (11:25-11:35)
  • PQC for IKEv2 in strongSwan - Leonie Bruckert (5 min) (11:35-11:40)
  • ESP Header Compression and Diet-ESP - Tobias Guggemos (10 min) (11:40-11:50)
  • Labeled IPsec - Paul Wouters (10 min) (11:50-12:00)
  • IKEv1 graveyard - Paul Wouters (5 min) (12:00-12:05)

• Other presentations
  • IP Traffic Flow Security - Christian Hopps (15 min) (12:05-12:20)
WG Status Report

In RFC Editor queue:
  draft-ietf-ipsecme-split-dns
Publication requested:
  draft-ietf-ipsecme-implicit-iv
WGLC done:
  draft-ietf-ipsecme-qr-ikev2
Work in progress:
  draft-ietf-ipsecme-ipv6-ipv4-codes
# draft-ietf-ipsecme-ipv6-ipv4-codes

## Current Design

<table>
<thead>
<tr>
<th>Requested @ Initiator</th>
<th>Supported @ Responder</th>
<th>Assigned @ Responder</th>
<th>Returned Notification Code</th>
<th>Initiator’s behavior receipt of the notification code</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv6</td>
<td>None</td>
<td>IP6_ONLY_ALLOWED</td>
<td>MUST NOT request IPv4 if supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MUST send a new request for IPv6 if supported</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
<td>IP6_ONLY_ALLOWED</td>
<td>MUST NOT request IPv4 if supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4</td>
<td>None</td>
<td>IP4_ONLY_ALLOWED</td>
<td>MUST NOT request IPv6 if supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MUST send a new request for IPv4 if supported</td>
</tr>
<tr>
<td>IPv4</td>
<td>IPv4</td>
<td>IPv4</td>
<td>IP4_ONLY_ALLOWED</td>
<td>MUST NOT request IPv6 if supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 or IPv6 (Policy-based)</td>
<td>IPv4 or IPv6</td>
<td>None</td>
<td>None</td>
<td>The initiator MAY send a request for the other AF</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4</td>
<td>IPv4</td>
<td>IP4_ONLY_ALLOWED</td>
<td>MUST NOT send a request for IPv6</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
<td>IP6_ONLY_ALLOWED</td>
<td>MUST NOT send a request for IPv4</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

The returned code reflects the capabilities of the responder. The code is blindly returned no matter what address is requested by the initiator. **Less processing** at the server.
### An Alternate Design

<table>
<thead>
<tr>
<th>Requested @ Initiator</th>
<th>Supported @ Responder</th>
<th>Assigned @</th>
<th>Returned Notification Code</th>
<th>Initiator’s behavior receipt of the notification code</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv6</td>
<td>None</td>
<td>ADDITIONAL_ADDRESS_FAMILY_POSSIBLE</td>
<td>MUST NOT request IPv4 MUST send a new request for IPv6 if supported</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
<td>None</td>
<td>MUST NOT request IPv4</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4</td>
<td>None</td>
<td>ADDITIONAL_ADDRESS_FAMILY_POSSIBLE</td>
<td>MUST NOT request IPv6 MUST send a new request for IPv4 if supported</td>
</tr>
<tr>
<td>IPv4</td>
<td>IPv4</td>
<td>IPv4</td>
<td>None</td>
<td>MUST NOT request IPv6</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4</td>
<td>IPv4</td>
<td>None</td>
<td>MUST NOT send a request for IPv6</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
<td>None</td>
<td>MUST NOT send a request for IPv4</td>
</tr>
<tr>
<td>IPv4 and IPv6 (Policy-based)</td>
<td>IPv4 or IPv6 (Policy-based)</td>
<td>IPv4 or IPv6</td>
<td>ADDITIONAL_ADDRESS_FAMILY_POSSIBLE</td>
<td>The initiator MAY send a request for the other AF</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Consumes **one code** instead of two.
The returned code is a function of the requested address type(s). **More processing** at the server.
What’s Next?

- Update the draft to record the WG consensus on the code(s) and ask for a WGLC
Work items

- Intermediate Exchange in the IKEv2 Protocol - Valery Smyslov
  - draft-smyslov-ipsecme-ikev2-aux
- Post-quantum Key Exchanges in IKEv2 - Valery Smyslov
  - draft-tjhai-ipsecme-hybrid-qske-ikev2
- An implementor's view on Hybrid PQKE in IKEv2 - Tobias Heider
- PQC for IKEv2 in strongSwan - Leonie Bruckert
- ESP Header Compression and Diet-ESP - Tobias Guggemos
  - draft-mglt-ipsecme-diet-esp
- Labeled IPsec - Paul Wouters
  - draft-ietf-ipsecme-labeled-ipsec
- IKEv1 graveyard - Paul Wouters
  - draft-pwouters-ikev1-ipsec-graveyard
- Other presentations
  - IP Traffic Flow Security - Christian Hopps
    - Draft-hopps-ipsecme-iptfs
Open Discussion

• Other points of interest?