Note Well

[https://www.ietf.org/about/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.

- 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/) 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)
IETF Virtual Meeting Tips

(we are all remote)

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended
IETF Code of Conduct (RFC 7154)

- “IETF participants extend respect and courtesy to their colleagues at all times.”
- Native English speakers “communicate clearly, including speaking slowly and limiting the use of slang”
- “reasoned argument rather than through intimidation or personal attack”
- “best solution for the whole Internet, not just the best solution for any particular network, technology, vendor, or user.”
- “Individuals are prepared to contribute to the ongoing work of the group”
Agenda

Signing

- v5→v6 (Keys, Sigs)
- v5 Signature trailer length field width
- v5 Signature salt size
- Context parameter for signatures

Encryption

- Context parameter for encryption
- Remove checksum from v5 PKESK

Overall

- Guidance for Designated Expert
- Spec title
- Meet in Yokohama (IETF 116)?
v5 → v6 (Keys, Sigs, OPS)

• Should we rename v5 sigs and keys to avoid conflict with GnuPG?
  - If so, also change prefix octet (for fingerprint and certification calculations): 0x9a → 0x9b?

• MR: !231

• [should we also move PKESK and SKESK to v6?]
Signature trailer length width field

<table>
<thead>
<tr>
<th>Version</th>
<th>Hashed data trailer suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>v3</td>
<td>Signed data...</td>
</tr>
<tr>
<td></td>
<td>sigtype</td>
</tr>
<tr>
<td></td>
<td>Signature timestamp</td>
</tr>
<tr>
<td>v4</td>
<td>Trailer...</td>
</tr>
<tr>
<td></td>
<td>0x04</td>
</tr>
<tr>
<td></td>
<td>0xff</td>
</tr>
<tr>
<td></td>
<td>Trailer length (in octets mod $2^{32}$)</td>
</tr>
<tr>
<td>v5</td>
<td>0x05</td>
</tr>
<tr>
<td></td>
<td>0xff</td>
</tr>
<tr>
<td></td>
<td>Trailer length (in octets mod $2^{64}$)</td>
</tr>
</tbody>
</table>

- A v5 signature can be transformed into a v3 type 0 or type 1 signature over different data (#130)
- Proposed: revert from 8-octet to 4-octet width field
- MR: !220
Length of Salt

PQ algorithms might want > 16 octets salt (see #150)

• Proposed: bind salt size to sig hash algorithm
  – Indicate salt size on wire?
  – What behavior if salt size doesn’t match algorithm?
  – What salt size is expected for deprecated hash algos?

• MR: !219
Context Parameter for Signatures

• Should v5 signing and verification include a context parameter?
  – If so, how does the signer know what context parameter to include?

• MR: !214
Context Parameter for Encryption

• Should SEIPDv2 encryption require choice of a context parameter?
  − If so, how does the signer know what context parameter to include?

• MR: !214
v5 ECDH PKESK: Remove Checksum and Padding?

<table>
<thead>
<tr>
<th>Version</th>
<th>ECDH Keywrap input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current (v3 and v5)</td>
<td>&lt;1o symalgo&gt;&lt;key&gt;&lt;2o checksum&gt;&lt;padding&gt;</td>
</tr>
<tr>
<td>Proposed (v5 only)</td>
<td>&lt;key&gt;</td>
</tr>
</tbody>
</table>

- ECDH keywrap has implicit checksum
- SEIPDv2 exposes symmetric algorithm
- All session keys are blocksize (multiples of 8 octets)
- Only ECDH, not other pubkey algos
- MR: !223
Document title

- "OpenPGP Message Format"
  - But not just messages

- Alternate titles?
  - OpenPGP
  - OpenPGP Protocol
  - OpenPGP Wire Format and Semantics
  - OpenPGP Messages, Signatures, Keys, and Certificates
  - OpenPGP Data Format
Next Steps?

• Done with WGLC?
• Meet in Yokohama?