Interop Testing v6

Justus Winter <justus@sequoia-pgp.org>

IETF 116, 2023-03-29

https://tests.sequoia-pgp.org

https://tests.sequoia-pgp.org/v6.html

A little Context, please?

- interop testing OpenPGP since 2019
- circa 114 tests
- around 1239 test vectors
- found loads of bugs across many different implementations
- improved implementations
- improved our understanding of the ecosystem
- highlights areas where implementations lack guidance
- feedback for the working group
- spin-off: *S*tateless *O*penPGP *P*rotocol (?)
Testing the Crypto Refresh!

- includes some v6 tests
  - test vectors from the draft
- [https://tests.sequoia-pgp.org](https://tests.sequoia-pgp.org)
  - tests released versions only
  - runs all tests
  - enter "v6" in the search bar
- [https://tests.sequoia-pgp.org/v6.html](https://tests.sequoia-pgp.org/v6.html)
  - happy to test your preview releases
  - runs only v6 tests

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>GnuPG 2.2.4</td>
<td>0.1.0</td>
</tr>
<tr>
<td>GnuPG 2.4.0</td>
<td>0.1.0</td>
</tr>
<tr>
<td>OpenPGP.js 5.5.0</td>
<td>sop-openssl 0.27.3</td>
</tr>
<tr>
<td>LibTDMC 1.4.0</td>
<td>1.2.0</td>
</tr>
<tr>
<td>GnuPG-1.12.0</td>
<td>sop-openssl 0.27.3</td>
</tr>
<tr>
<td>GnuPG-1.4.23</td>
<td>sop-openssl 0.27.3</td>
</tr>
<tr>
<td>GnuPG-1.4.23</td>
<td>sop-openssl 0.27.3</td>
</tr>
<tr>
<td>GnuPG-1.4.23</td>
<td>sop-openssl 0.27.3</td>
</tr>
<tr>
<td>RNP-0.16.2</td>
<td>0.2.0</td>
</tr>
<tr>
<td>OpenPGP.js 5.5.0</td>
<td>sop-openssl 0.27.3</td>
</tr>
<tr>
<td>OpenPGP.js 5.5.0</td>
<td>sop-openssl 0.27.3</td>
</tr>
<tr>
<td>Bouncy Castle 1.72</td>
<td>PGPainless-SO...</td>
</tr>
</tbody>
</table>
What can you do?

- suggest tests, write tests, review tests
- help with test suite development and maintenance
- implementers:
  - tell me how to get/build/update your SOP frontend
  - do you have a development version?
  - implement ‘–profile’
  - consider implementing your own SOP frontend
    - if you do, clue me how to keep it up-to-date
    - preferably, get it into Debian
- get in touch

Justus Winter <justus@sequoia-pgp.org>