IMPROVEMENTS AROUND DOCUMENT SIGNATURES AND ENCRYPTION

SAMUEL MEHRBRODT, CIB
FOSDEM 2018
CONTENT

1. SIGNATURE LINES
2. OPENPGP SUPPORT
1. SIGNATURE LINES
SIGNATURE LINES

• Visual representation of document signature
• Combine handwritten signature and digital signature
• LibreOffice 6.0:
  – OOXML Import
• LibreOffice 6.1
  – OOXML Roundtrip (Export added)
  – ODF Export (Import tbd)
  – Generate new Signature Lines
  – Digitally sign Signature Lines (tbd)
OPENPGP SUPPORT
OPENPGP SUPPORT

• Signing with OpenPGP keys
  – Since LibreOffice 5.4: Linux only
  – Since LibreOffice 6.0: Linux, macOS and Windows
  – ODF-conformant

• Encrypting with OpenPGP keys
  – LibreOffice 6.0: Linux, macOS and Windows
  – Extension to ODF, proposed to OASIS ODF TC

• Currently the only ODF consumer implementing OpenPGP
HOW DOES IT WORK?

GnuPG

GPG4Win

Kleopatra

Seahorse

IPC / execve

gpgme

LibreOffice

ODF
### Select Certificate

Select the certificate you want to use for signing:

<table>
<thead>
<tr>
<th>Issued to</th>
<th>Issued by</th>
<th>Type</th>
<th>Expiration date</th>
<th>Certificate usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibreOffice Build Team (CC</td>
<td>CA Cert Signing Authority</td>
<td>X.509</td>
<td>05/16/2010</td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
<tr>
<td>thb backup &lt;me@localhos</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td></td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
<tr>
<td>Thorsten Behrens &lt;thb@d</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td></td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
<tr>
<td>Thorsten Behrens (private</td>
<td>OpenPGP</td>
<td>11/22/2018</td>
<td></td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
<tr>
<td>dfgdafgfdg (test key) &lt;tho</td>
<td>OpenPGP</td>
<td>11/22/2018</td>
<td></td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
<tr>
<td><a href="mailto:foo@bar.de">foo@bar.de</a></td>
<td>OpenPGP</td>
<td>03/13/2025</td>
<td></td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
<tr>
<td><a href="mailto:foo@bar.de">foo@bar.de</a></td>
<td>OpenPGP</td>
<td>05/24/2017</td>
<td></td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
<tr>
<td><a href="mailto:foo@bar.de">foo@bar.de</a></td>
<td>OpenPGP</td>
<td>05/30/2017</td>
<td></td>
<td>Digital signature, Non-repudiation, Key encryption, Data encryption</td>
</tr>
</tbody>
</table>

---

**NO EXTRA KEY STORE**
UI IMPROVEMENTS
THE END

→ QUESTIONS?

... THANKS TO:

Bundesamt für Sicherheit in der Informationstechnik