GPG4LIBRE: OPENPGP SIGNING & ENCRYPTION IN LIBREOFFICE

LIBREOFFICE CONFERENCE ROME
OCTOBER 12TH, 2017

Thorsten.Behrens@cib.de
GPG4LIBRE - MOTIVATION

• we don’t do enough crypto yet!
• put encryption and signing at user’s finger tips
• use something that’s
  – cheap
  – ubiquitous
  – peer to peer
  – stable, reliable, cross-platform, and comes with tons of features
ARCHITECTURE

GnuPG

IPC / execve

freedesktop.org

LibreOffice

Seahorse

Kleopatra

gpgme

GPG\4WIN

CIB software

ODF™
LibreOffice process
soffice.bin

Kleopatra/GPA/Seahorse process
seahorse

GnuPG process
gpg

Start Certificate Manager

Manage trust levels, edit keys

gpgme_op_sign

gpgme_op_encrypt

...
UI IMPROVEMENTS
INTEGRATING ALL AVAILABLE KEYS

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>CACert WoT User</td>
<td>CA Cert Signing Authority</td>
<td>X.509</td>
<td>05/16/2010</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
</tr>
<tr>
<td>Thorsten Behrens &lt;th.behr&gt;</td>
<td>OpenPGP</td>
<td>01/16/2007</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td>Thorsten Behrens &lt;th.behr&gt;</td>
<td>OpenPGP</td>
<td>01/01/2010</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td>Thorsten Behrens &lt;thb@o</td>
<td>OpenPGP</td>
<td>02/16/2013</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>05/05/2014</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
</tr>
<tr>
<td>LibreOffice Build Team (CC</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td>thb backup &lt;me@localhos</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td>Thorsten Behrens &lt;thb@d</td>
<td>OpenPGP</td>
<td>11/22/2018</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td>Thorsten Behrens (private</td>
<td>OpenPGP</td>
<td>11/22/2018</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td>dfgdafgdfl (test key) &lt;tho</td>
<td>OpenPGP</td>
<td>03/13/2025</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:foo@bar.de">foo@bar.de</a></td>
<td>OpenPGP</td>
<td>05/24/2017</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:foo@bar.de">foo@bar.de</a></td>
<td>OpenPGP</td>
<td>05/30/2017</td>
<td>Digital signature, Non-repudiation, Key encryption</td>
<td></td>
</tr>
</tbody>
</table>

- Click on the "Start Certificate Manager..." button to proceed with certificate selection.
DEFER TO PLATFORM WHERE USEFUL
Based on: https://www.w3.org/TR/xmldsig-core/

```xml
<SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
  <Reference URI="styles.xml">
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <DigestValue>h8x5UxEL9t9W8UfYEHeLme1J0qpke+H7AaGGFD8qzFY=</DigestValue>
  </Reference>
</SignedInfo>
</Signature>
```
Actual OpenPGP-Signature:

```xml
<SignatureValue>LS0tLS1CRUdJ...tLS0tCg==</SignatureValue>
<KeyInfo>
  <PGPData>
    <PGPKeyID>OTA5QkUyNTc1Q0VEQkVBMw==</PGPKeyID>
    <PGPKeyPacket>LS0tLS1C...S0tCg==</PGPKeyPacket>
  </PGPData>
</KeyInfo>
```
ENCRIPTION

- extended save dialog
ENCRYPTION

- pick recipient

<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>FreeBSD Security O</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Conectiva S.A.</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Wichert Akkerman</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Mark Cox &lt;mic@rec</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Kevin E. Fu &lt;fubob@</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Werner Koch (gnupg)</td>
<td>OpenPGP</td>
<td>12/31/2005</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Sun Security Coordl</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Steve Birnbaum &lt;sbi</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>security-officer@ne</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>IBM-ERS Team &lt;ersi</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Vladislav V. Mikhailc</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Damir Rajnovic (CISi)</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>Steve Fallin &lt;Steve.l</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
<tr>
<td>CIB Security &lt;Steve.l</td>
<td>OpenPGP</td>
<td>00/00/0000</td>
<td>Digital signature, Non-repudiation, Key exchange</td>
<td></td>
</tr>
</tbody>
</table>
Encryption based on: https://www.w3.org/TR/2002/REC-xmlenc-core-20021210

```xml
<manifest:manifest xmlns:manifest="urn:oasis..." manifest:version="1.2"
manifest:loext="urn:org:do...">
  <loext:KeyInfo>
    <loext:EncryptedKey>
      <loext:EncryptionMethod loext:Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
      <loext:KeyInfo>
        <loext:PGPData>
          <loext:PGPKeyID>QjE3...5NA==</loext:PGPKeyID>
          <loext:PGPKeyPacket>LS0tLS0tLS0K</loext:PGPKeyPacket>
        </loext:PGPData>
        </loext:KeyInfo>
      <loext:CipherData>
        <loext:CipherValue>FAm4B...aB8=</loext:CipherValue>
      </loext:CipherData>
    </loext:EncryptedKey>
  </loext:KeyInfo>
  <manifest:file-entry manifest:full-path="/" manifest:version="1.2"
manifest:media-type="application/vnd.oasis.opendocument.text"/>
</manifest:manifest>
```
MARKUP: XML ENCRYPTION

File entry (details might still change):

```xml
<manifest:file-entry manifest:full-path="content.xml" manifest:media-type="text/xml" manifest:size="15781">
  <manifest:encryption-data manifest:checksum-type="urn:oasis:names:tc:opendocument:xmlns:manifest:1.0#sha256-1k">
    <manifest:algorithm-manifest:algorithm-name="http://www.w3.org/2001/04/xmlenc#aes256-cbc" manifest:initialisation-vector="0jF3LtJHWJr/j9UvipYwQ=="/>
  </manifest:encryption-data>
</manifest:file-entry>
```
GPG4LIBRE – WRAP-UP AND Q&A
ROADMAP

- ODF-conformant signing on Linux
  - ships with LibreOffice 5.4

- ODF-conformant signing also on Windows
  - planned for LibreOffice 6.0 (Feb. 2018)
  - also planned for OS X – open for Android

- experimental encryption on Linux & Windows
  - planned for LibreOffice 6.0 (Feb. 2018)
  - needs ODF extensions

- ODF-next
  - proposing XMLSEC-extensions for OpenPGP encryption to OASIS ODF TC – GA around 2018 or 2019
THANK YOU!

OUR PRODUCTS:
HTTP://LIBREOFFICE.CIB.DE/

WE CAN HELP:
HTTP://LIBREOFFICE.CIB.DE/SUPPORT