
GPG4LIBRE: OPENPGP SIGNING & ENCRYPTION IN LIBREOFFICE

LIBREOFFICE CONFERENCE ROME
OCTOBER 12TH, 2017

Thorsten.Behrens@cib.de



Bundesamt
für Sicherheit in der
Informationstechnik



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



Bundesamt
für Sicherheit in der
Informationstechnik

CIB
software



⋮



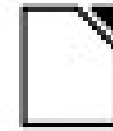
Seahorse

⋮

IPC / execute



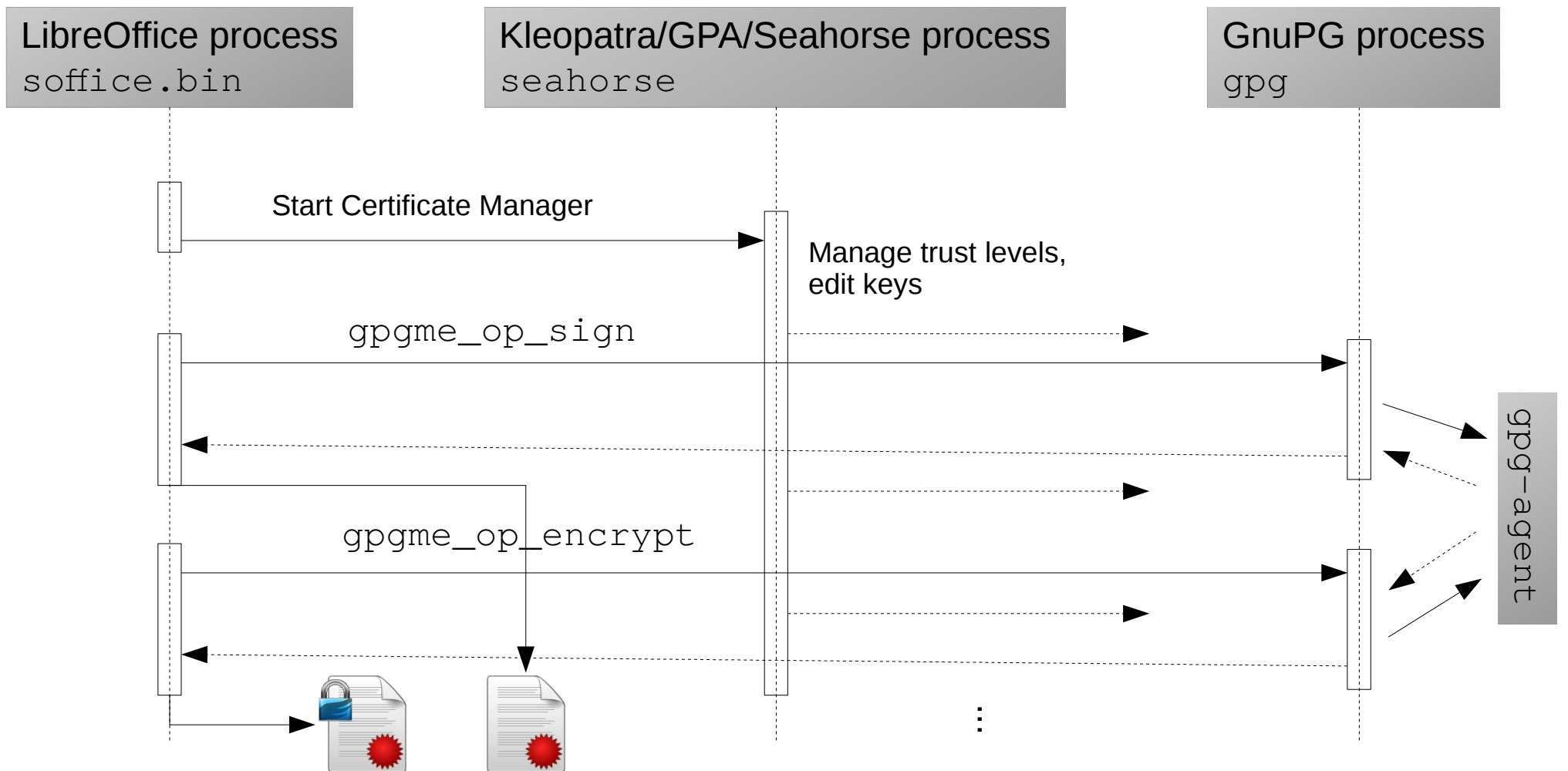
gpgme



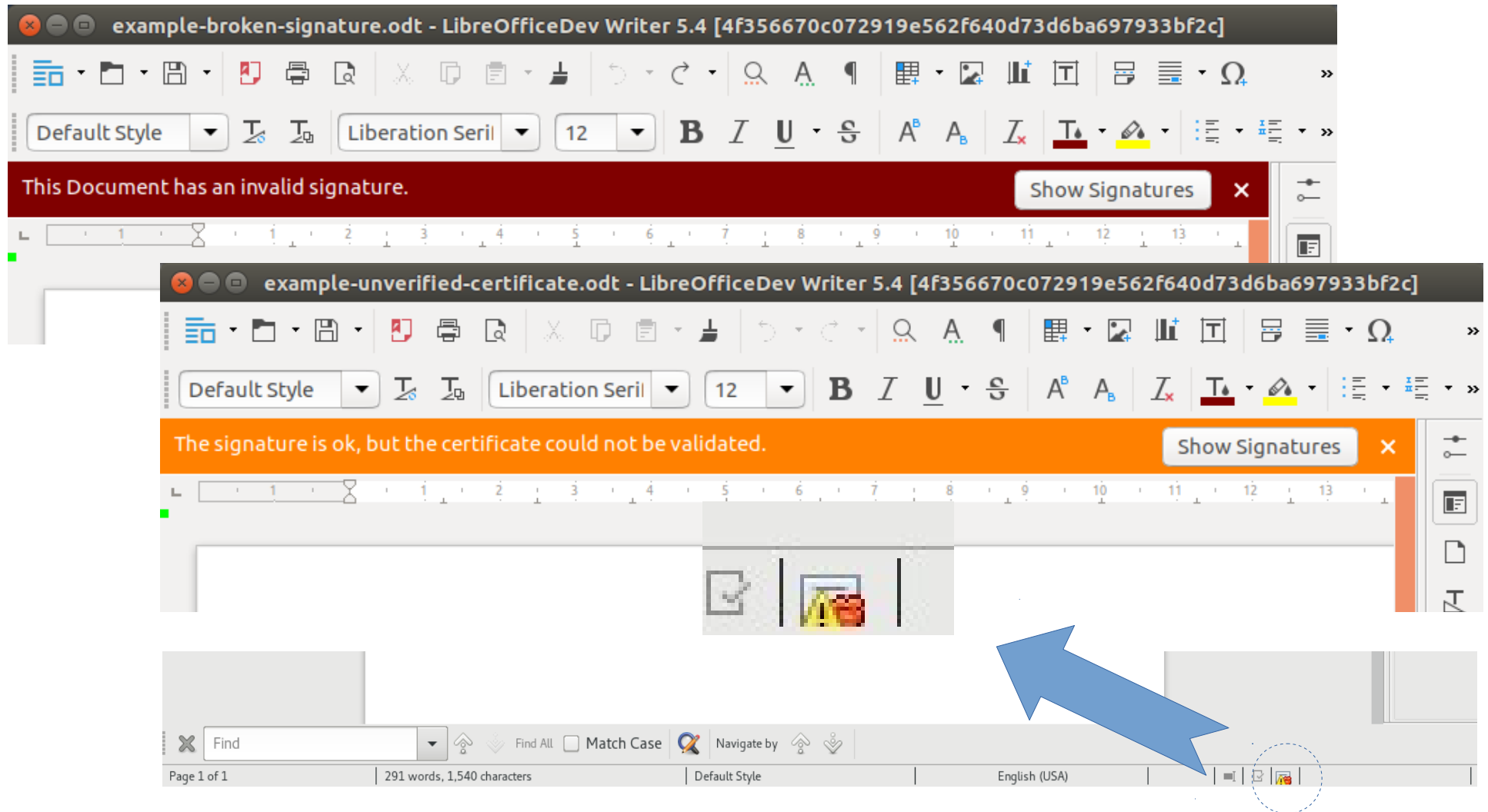
LibreOffice
The Document Foundation



SEQUENCE DIAGRAM



UI IMPROVEMENTS



INTEGRATING ALL AVAILABLE KEYS



Bundesamt
für Sicherheit in der
Informationstechnik

CIB
software

Select Certificate

Select the certificate you want to use for signing:

Issued to	Issued by	Type	Expiration date	Certificate usage
LibreOffice Build Team (CC	Allgeier IT Solutions eVer	X.509	05/19/2017	Digital signature, Key encipherment, Data e
CAcert WoT User	CA Cert Signing Authority	X.509	05/16/2010	Digital signature, Non-repudiation, Key enci
	Thorsten Behrens <th.behr	OpenPGP	01/16/2007	Digital signature, Non-repudiation, Key enci
	Thorsten Behrens <th.behr	OpenPGP	01/01/2010	Digital signature, Non-repudiation, Key enci
	Thorsten Behrens <thb@o	OpenPGP	02/16/2013	Digital signature, Non-repudiation, Key enci
		OpenPGP	05/05/2014	Digital signature, Non-repudiation, Key enci
	LibreOffice Build Team (CC	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key enci
	thb backup <me@localhos	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key enci
	Thorsten Behrens <thb@d	OpenPGP	11/22/2018	Digital signature, Non-repudiation, Key enci
	Thorsten Behrens (private	OpenPGP	11/22/2018	Digital signature, Non-repudiation, Key enci
	dfgdafgdg (test key) <tho	OpenPGP	03/13/2025	Digital signature, Non-repudiation, Key enci
	<foo@bar.de>	OpenPGP	05/24/2017	Digital signature, Non-repudiation, Key enci
	<foo@bar.de>	OpenPGP	05/30/2017	Digital signature, Non-repudiation, Key enci

Remove

Start Certificate Manager...

Close

DEFER TO PLATFORM WHERE USEFUL



Bundesamt
für Sicherheit in der
Informationstechnik



The screenshot displays a Linux desktop environment with the 'Passwords and Keys' application open. The application shows a list of PGP keys, including Thorsten Behrens and Tiberiu-Cezar Tehnoetic. A 'pinentry-qt4' dialog box is overlaid on the screen, requesting a passphrase to unlock an OpenPGP secret key for 'Sweet Bubble <bubli@bubli.org>'. The dialog box shows the key details: '2048-bit RSA key, ID 681CC4E6D032BD91, created 2017-07-13'. The passphrase field contains three asterisks. A 'Certificate could not be validated' error message is also visible in the bottom left corner.

Issued by	Type	Expiration date	Certificate usage
Katarína Machálková <K.Machalkova@pod.cvut.c...	OpenPGP	00/00/0000	Digital signature, Non-...
Sweet Bubble <bubli@bubli.org>	OpenPGP	00/00/0000	Digital signature, Non-...

MARKUP: XML SIGNATURES



Bundesamt
für Sicherheit in der
Informationstechnik

CIB
software

Based on: <https://www.w3.org/TR/xmlsig-core/>

```
<Signature xmlns="http://www.w3.org/2000/09/xmlsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlsig-more#rsa-sha256"/>
    <Reference URI="styles.xml">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-core#sha256"/>
      <DigestValue>h8x5UxEL9t9W8UfYEHeLme1J0qpke+H7AaGGFD8qzFY=</DigestValue>
    </Reference>
  </SignedInfo>
</Signature>
```


MARKUP: XML SIGNATURES



Bundesamt
für Sicherheit in der
Informationstechnik

CIB
software

Actual OpenPGP-Signature:

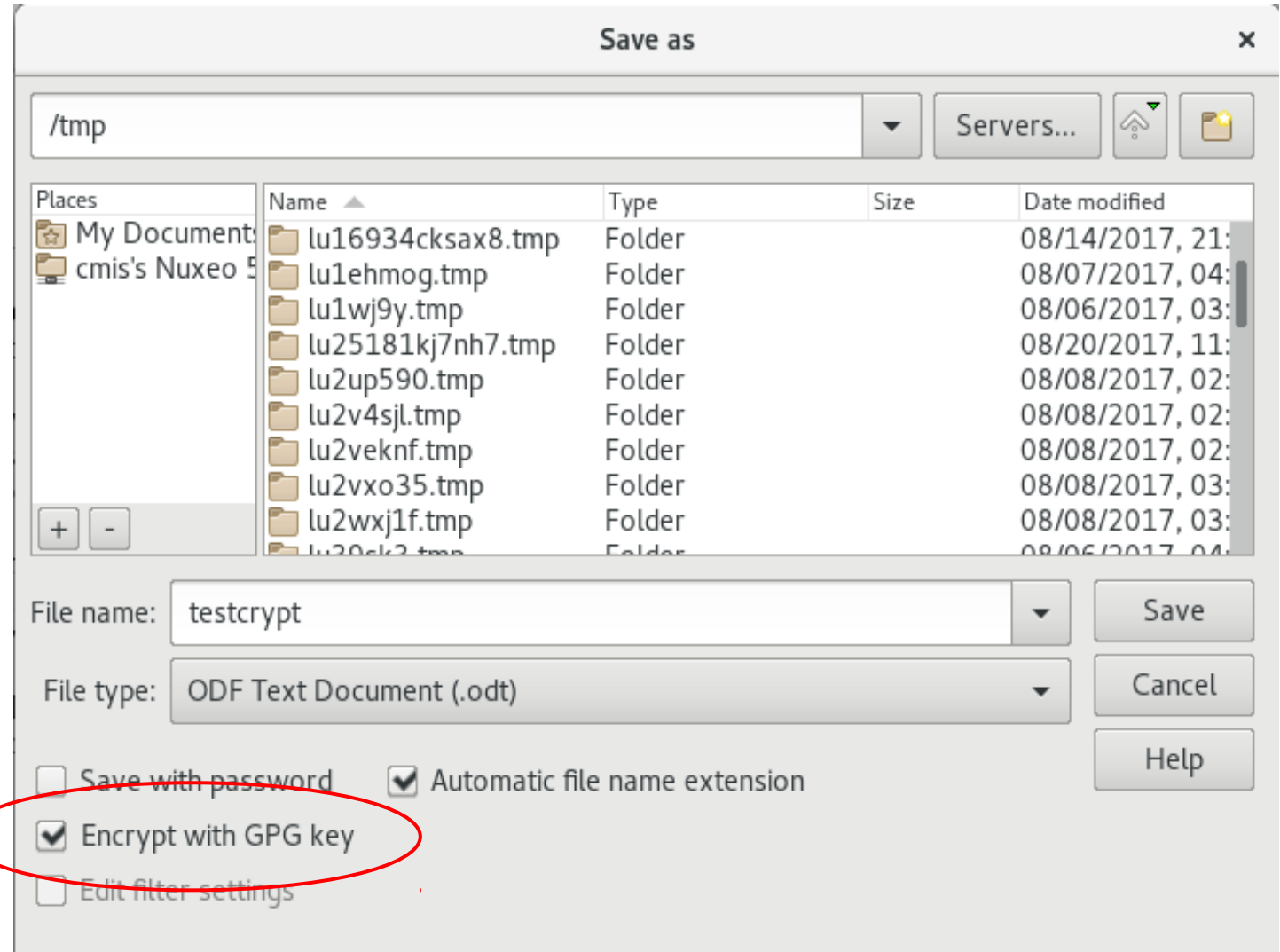
```
<SignatureValue>LS0tLS1CRUdJ...tLS0tCg==</SignatureValue>  
<KeyInfo>  
  <PGPData>  
    <PGPKeyID>OTA5QkUyNTc1Q0VEQkVBMw==</PGPKeyID>  
    <PGPKeyPacket>LS0tLS1C...S0tCg==</PGPKeyPacket>  
  </PGPData>  
</KeyInfo>
```

GPG4LIBRE - ENCRYPTION

ENCRYPTION



- extended save dialog



ENCRYPTION



- pick recipient

Select Certificate				
Select the certificate you want to use for signing:				
Issued to	Issued by	Type	Expiration date	Certificate usage
	FreeBSD Security O	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Conectiva S.A. <seci	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Wichert Akkerman <	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Mark Cox <mjc@rec	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Kevin E. Fu <fubob@	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Werner Koch (gnupg	OpenPGP	12/31/2005	Digital signature, Non-repudiation, Key en
	Sun Security Coordi	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Steve Birnbaum <sbi	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	security-officer@ne	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	IBM-ERS Team <ers	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Vladislav V. Mikhailc	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Damir Rajnovic (CIS	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	Steve Fallin <Steve.l	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en
	SSI Security S	OpenPGP	00/00/0000	Digital signature, Non-repudiation, Key en

MARKUP: XML ENCRYPTION



Bundesamt
für Sicherheit in der
Informationstechnik

CIB
software

Encryption based on: <https://www.w3.org/TR/2002/REC-xmlenc-core-20021210>

```
<manifest:manifest xmlns:manifest="urn:oasis..." manifest:version="1.2"
xmlns: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>LS0tL...LS0K</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"/>
```

MARKUP: XML ENCRYPTION



Bundesamt
für Sicherheit in der
Informationstechnik

CIB
software

File entry (details might still change):

```
<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:checksum="bbpZzvw+p0u+BAMI0wsxn0Bbs0n3P3oABCD9IGxKqyg=">  
    <manifest:algorithm manifest:algorithm-  
name="http://www.w3.org/2001/04/xmlenc#aes256-cbc"  
manifest:initialisation-vector="0jF3LtJHWJr/j9UvipYw0Q==" />  
  </manifest:encryption-data>  
</manifest:file-entry>
```

GPG4LIBRE – WRAP-UP AND Q&A

ROADMAP



Bundesamt
für Sicherheit in der
Informationstechnik



- 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!



**Bundesamt
für Sicherheit in der
Informationstechnik**

CIB
software

OUR PRODUCTS:

[HTTP://LIBREOFFICE.CIB.DE/](http://libreoffice.cib.de/)

WE CAN HELP:

[HTTP://LIBREOFFICE.CIB.DE/SUPPORT](http://libreoffice.cib.de/support)

