CIB software

GPG4LIBRE: OPENPGP SIGNING & ENCRYPTION IN LIBREOFFICE

LIBREOFFICE CONFERENCE ROME
OCTOBER 12TH, 2017

Thorsten.Behrens@cib.de

Bundesamt
für Sicherheit in der
Informationstechnik

LibreOffice
The Document Foundation

ROME - IT - MMXVII
CONFERENCE

GPG4LIBRE - MOTIVATION

Bundesamt für Sicherheit in der Informationstechnik

CIB software

- 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

GnuPG

⋮

GPG4WiN

Seahorse

⋮

IPC / execve

gpgme

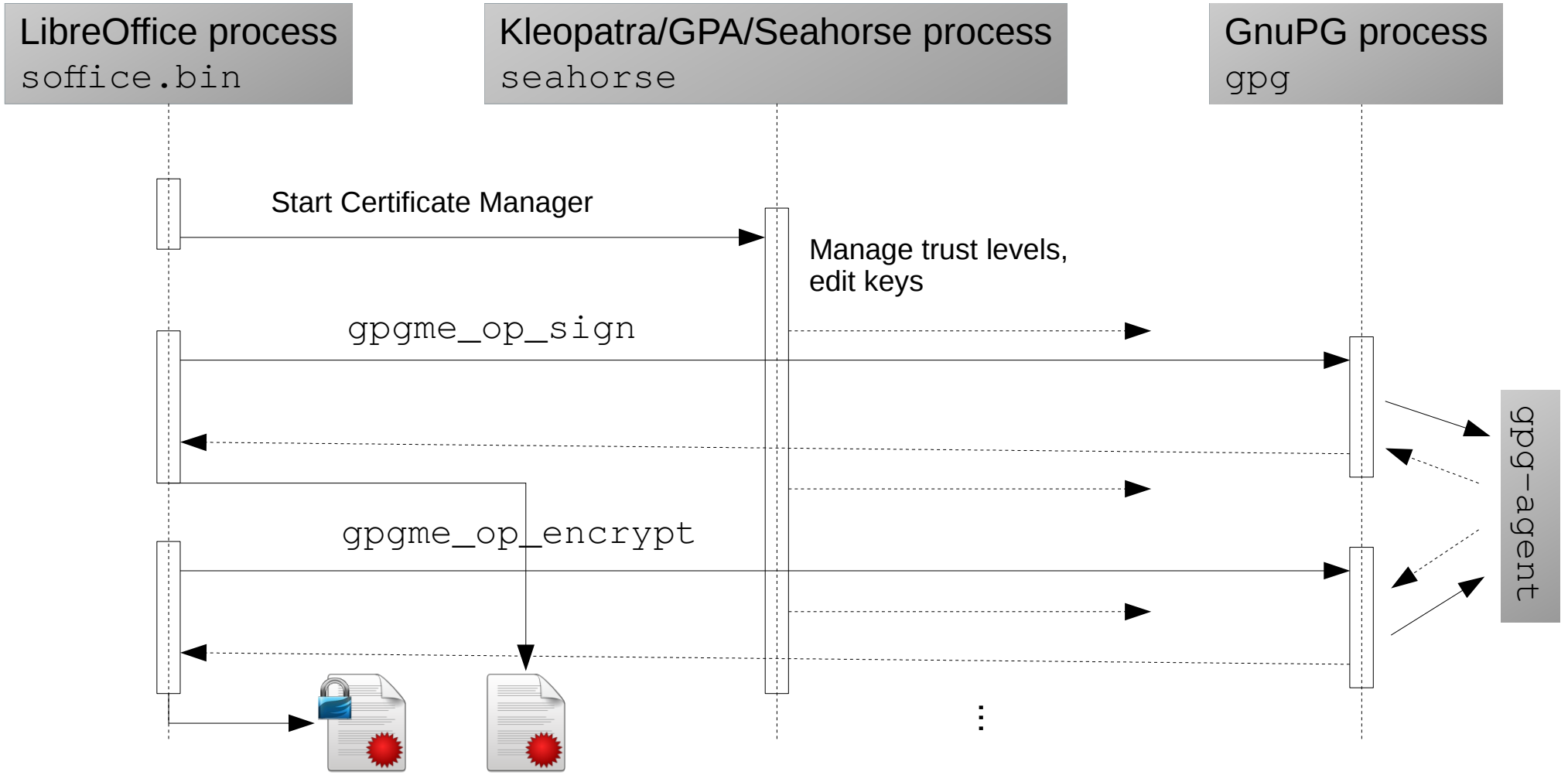
LibreOffice
The Document Foundation

ODF™

SEQUENCE DIAGRAM

Bundesamt für Sicherheit in der Informationstechnik

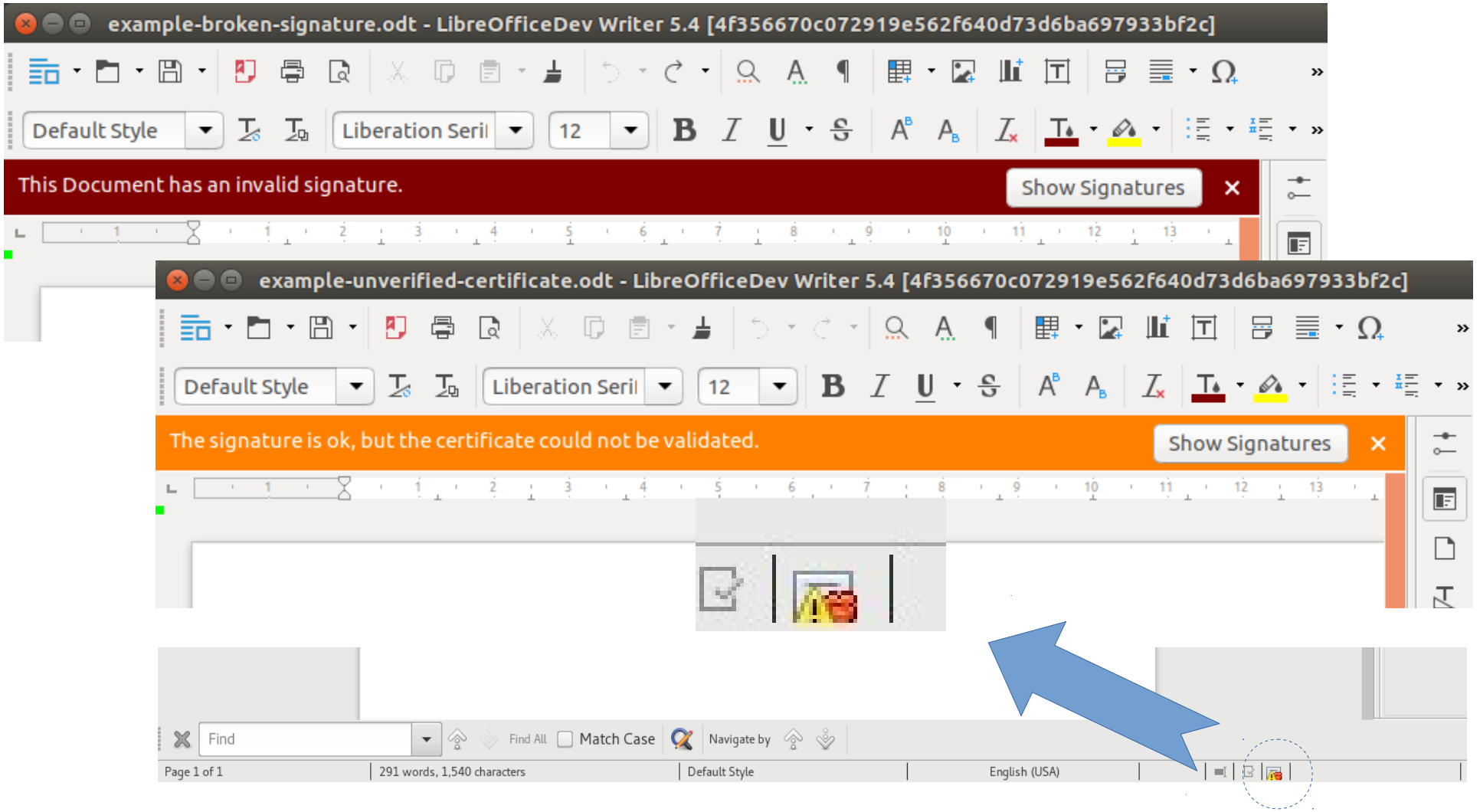
CIB software



UI IMPROVEMENTS

Bundesamt für Sicherheit in der Informationstechnik

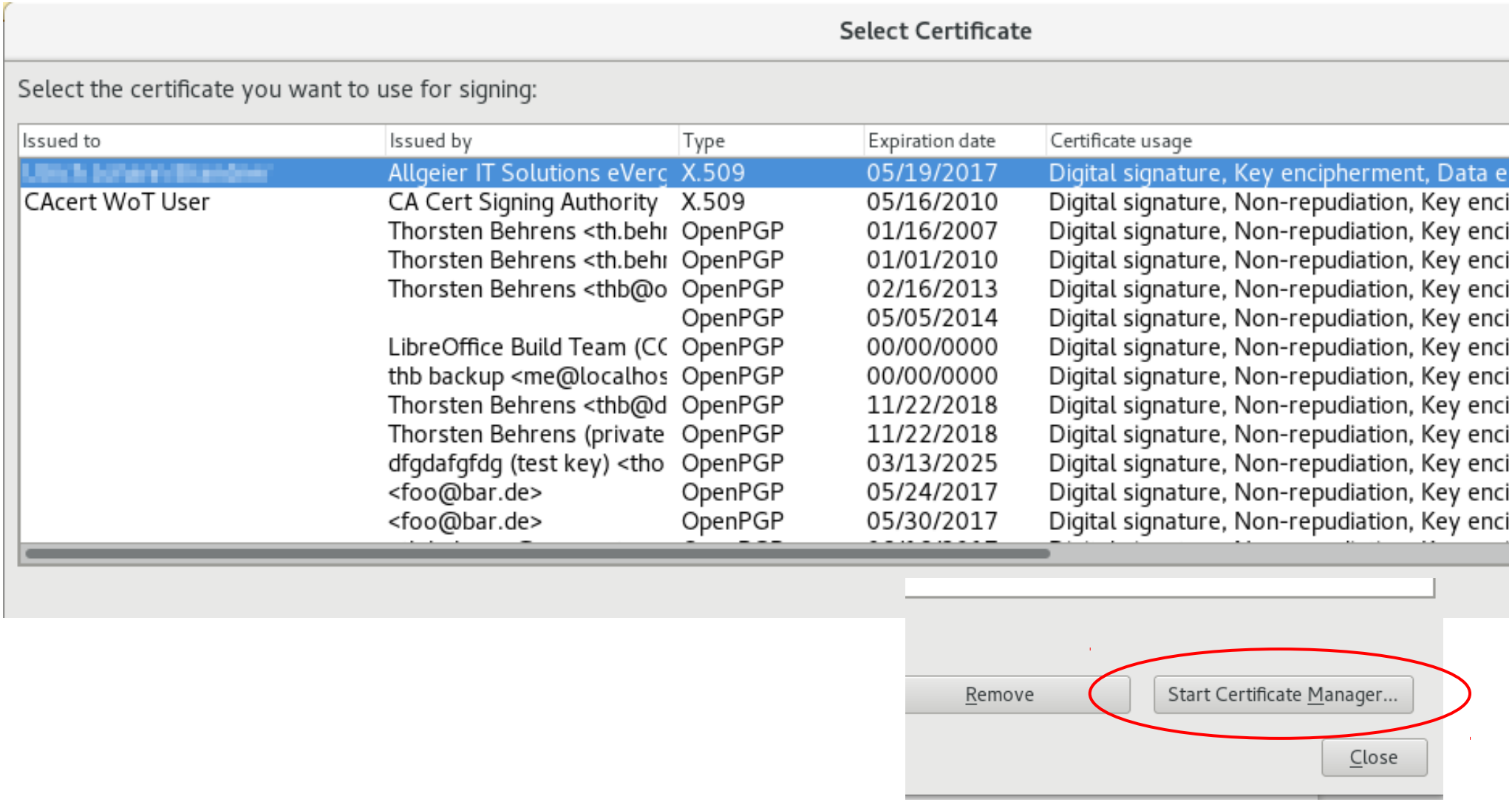
CIB software



INTEGRATING ALL AVAILABLE KEYS

Bundesamt für Sicherheit in der Informationstechnik

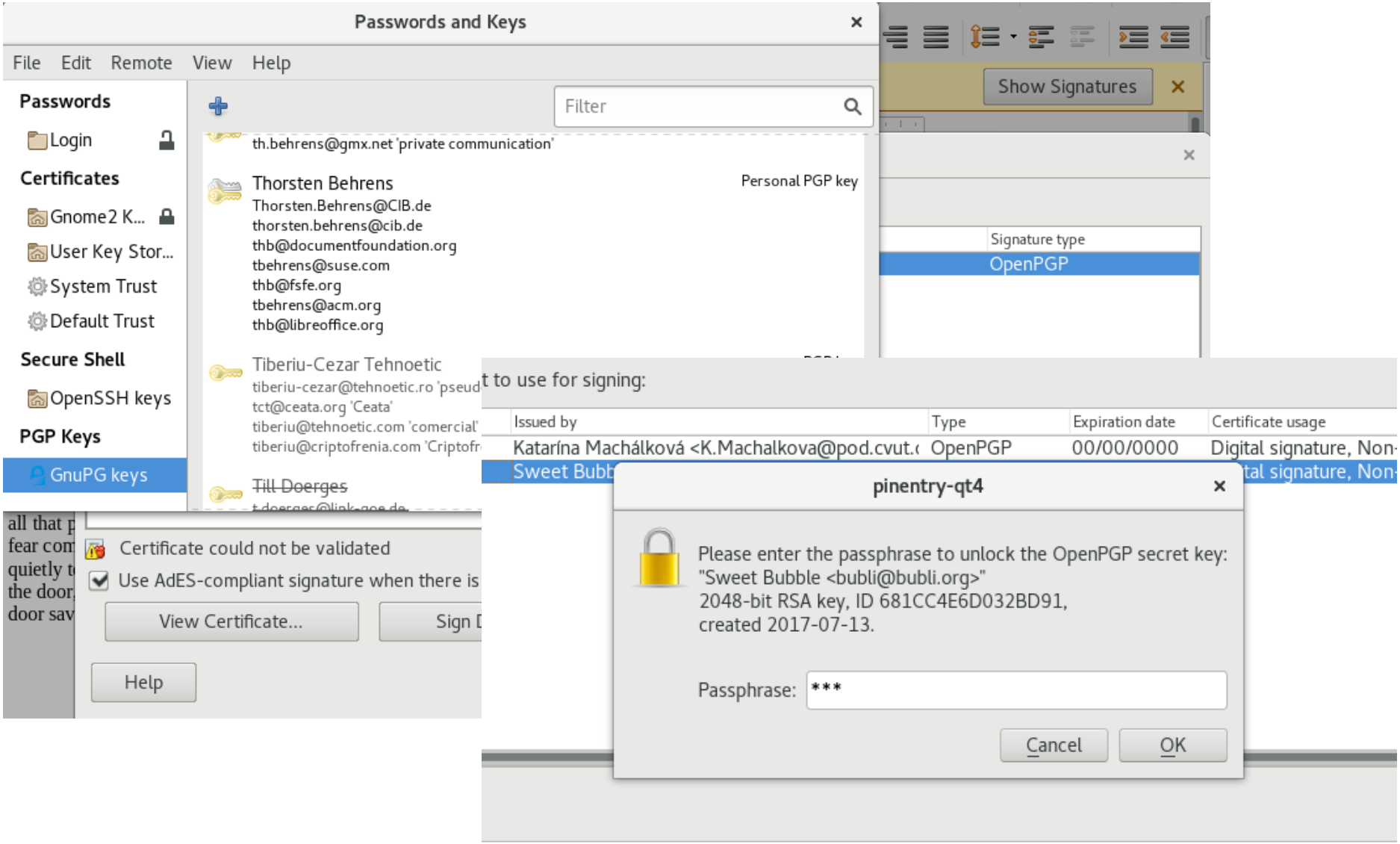
CIB software



DEFER TO PLATFORM WHERE USEFUL

Bundesamt für Sicherheit in der Informationstechnik

CIB software



MARKUP: XML SIGNATURES

Bundesamt für Sicherheit in der Informationstechnik

CIB software

Based on: https://www.w3.org/TR/xmldsig-core/

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"">
  <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">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>h8x5UxEL9t9W8UfYEHeLme1JOqpke+H7AaGGFD8qzFY=</DigestValue>
    </Reference>
```

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>
```

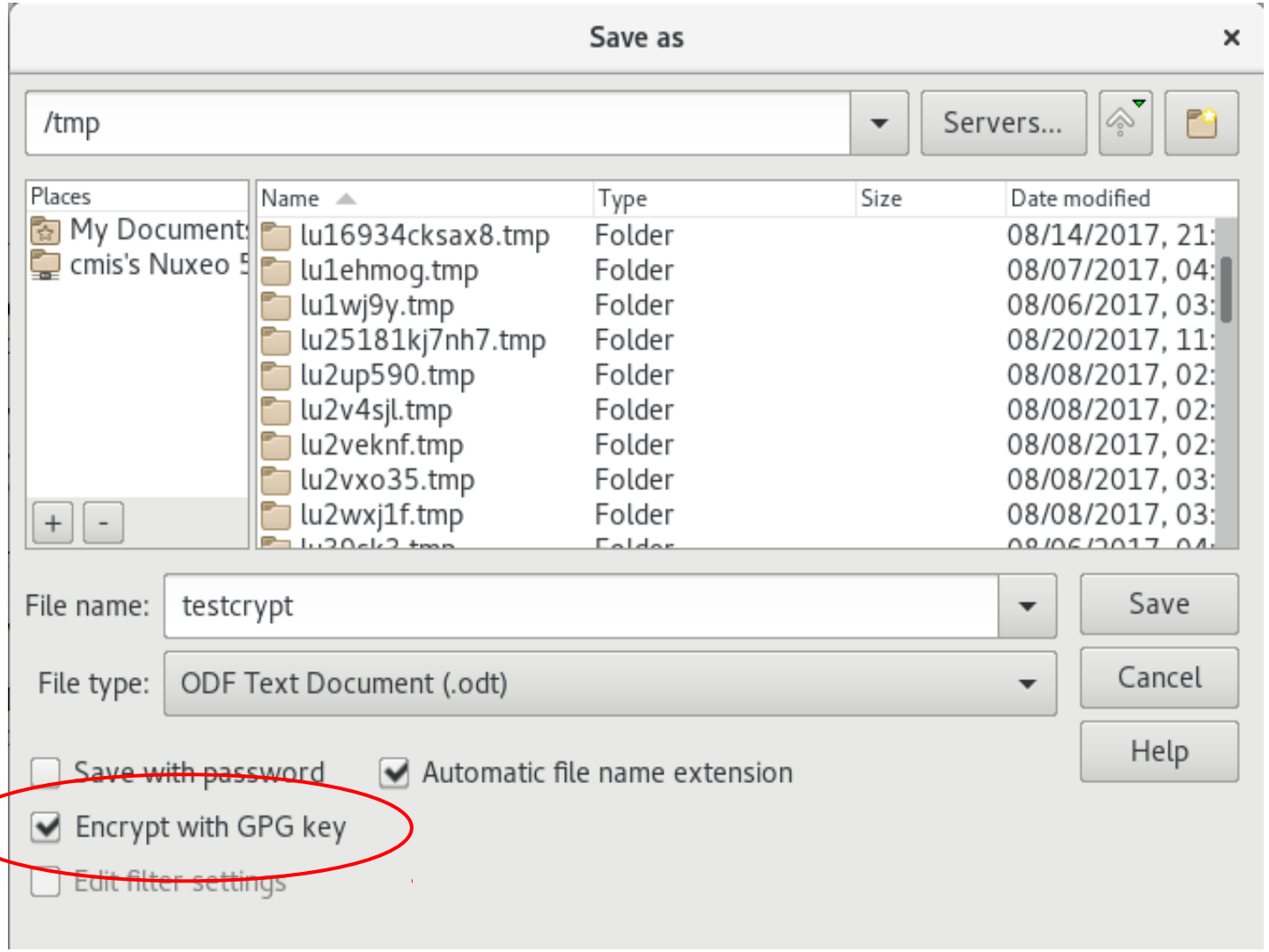
GPG4LIBRE - ENCRYPTION

ENCRYPTION

Bundesamt für Sicherheit in der Informationstechnik

CIB software

- extended save dialog

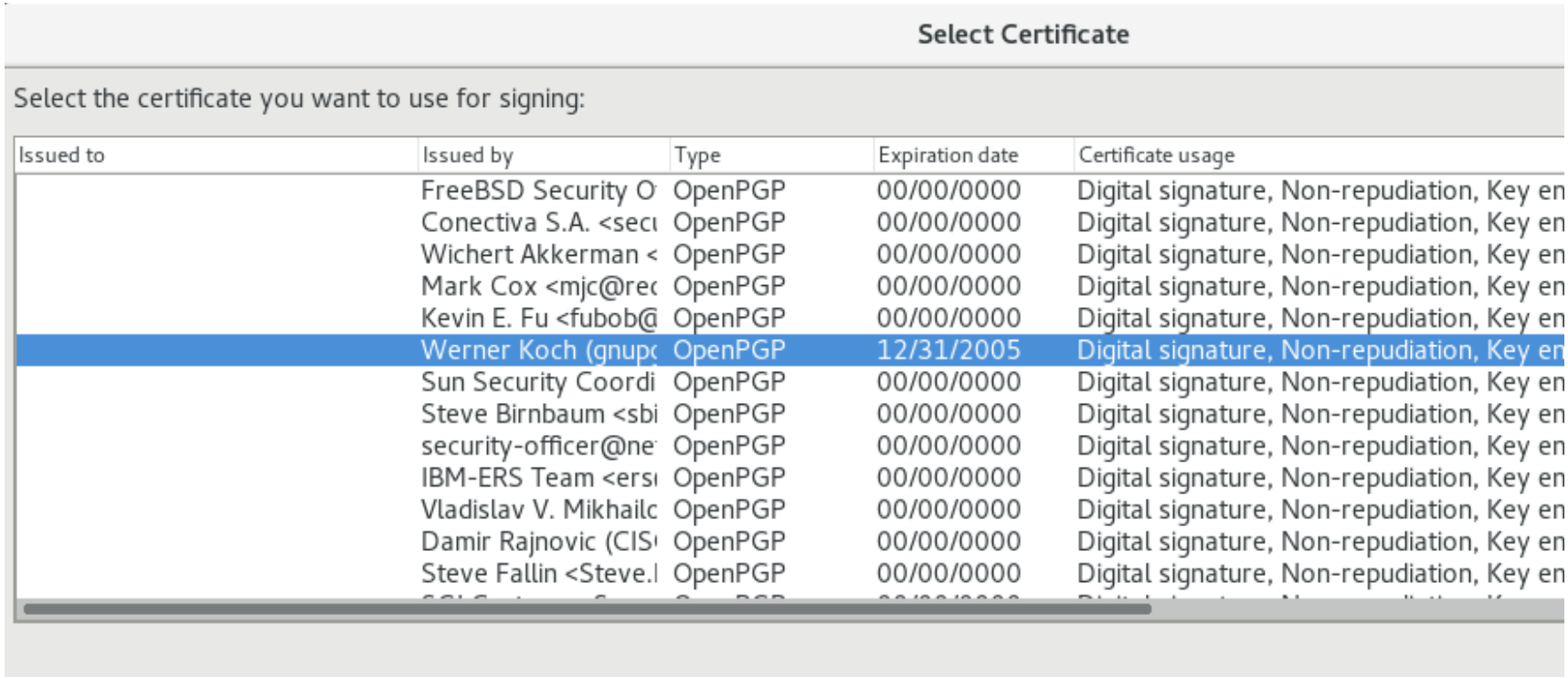


ENCRYPTION

Bundesamt für Sicherheit in der Informationstechnik

CIB software

- pick recipient



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+pOu+BAMI0wsxn0BbsOn3P3oABCd9IGxKqyg=">
  <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

CIB software

- 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/

WE CAN HELP:

HTTP://LIBREOFFICE.CIB.DE/SUPPORT