CIB software

DIGITAL SIGNATURE AND ENCRYPTION WORKFLOWS WITH LIBREOFFICE

FrOSCon 2018

Thorsten.Behrens@cib.de

LiMux

Die IT-Evolution

Bundesamt
für Sicherheit in der
Informationstechnik

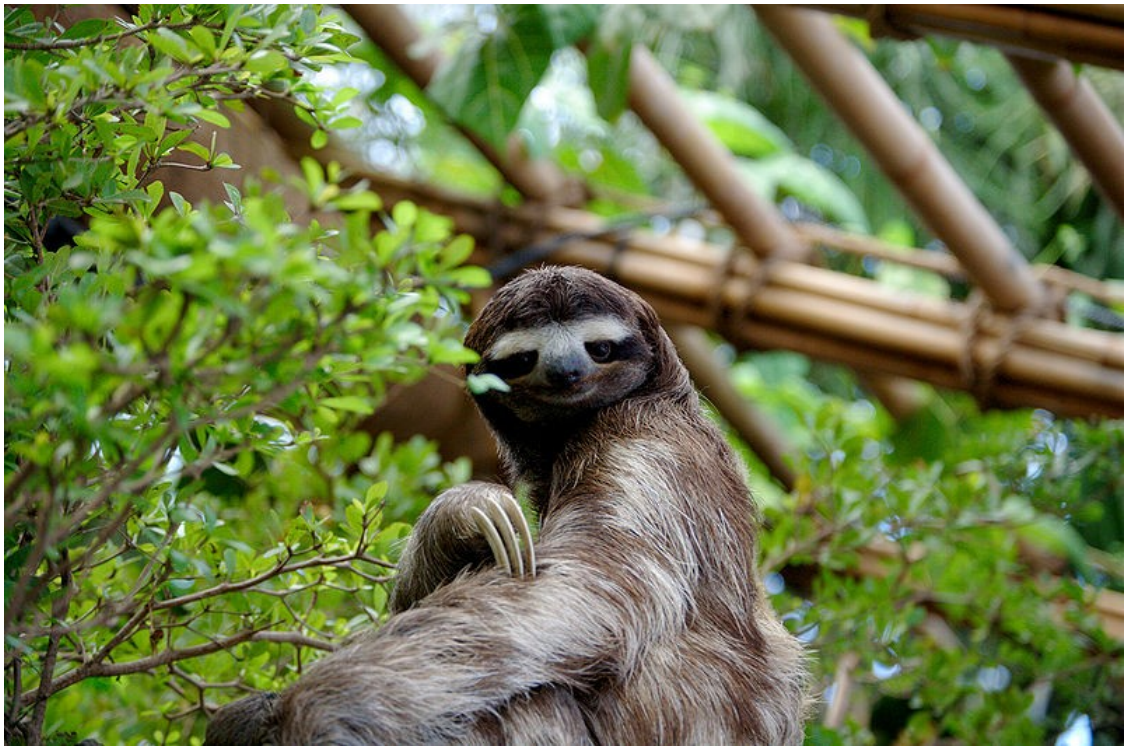
Who am I?

Thorsten Behrens

- since 2015 working for CIB, built our LibreOffice team
- one of the LibreOffice ~~forkers~~/founders, on the board of the foundation
- working on LibreOffice/OpenOffice code since 2001
- hacker, computer scientist, rooting for open source & open standards

It's 2018, y'all!

- it's 2018, and Germany is waking up to digitalisation :)



- ..and now, what can we do with free software?

First off, some background

Alphabet soup of standards

- AdES: https://en.wikipedia.org/wiki/Advanced_electronic_signature
  - PAdES (pdf)
  - XAdES (xml)
  - CAdES (CMS, e.g. s/mime)
  - for the EU: eIDAS - conforming to regulations for PDF signing https://en.wikipedia.org/wiki/EIDAS

A bit of history

- things started in Germany with signaturgesetz from 1997
- which subsequently got replaced by the EU eIDAS regulation in 2016 (with the VDG (Vertrauensdienstegesetz as auxiliary))
- (though eIDAS came into force in 2014 already)
- VDG permits personal certs, and org certs ("Siegel")
- with that the initial, very strict requirements got softened
- e.g. electronic invoices now valid even w/o qualified digital signature

..but:

- *but* - qualified signature helps a lot, in that it has prima facie authenticity
- by now, electronic signatures have been made equivalent (and therefore electronic document interchange) with paper-based contracts in Germany:
  - BGB 126a - https://www.buzer.de/s1.htm?g=BGB&a=126a
  - VwVfG 3a - https://www.buzer.de/s1.htm?g=VwVfG&a=3a
  - ZPO 130a - https://www.buzer.de/s1.htm?g=ZPO&a=130a
  - and ZPO 371a - https://www.buzer.de/s1.htm?g=ZPO&a=371a on authenticity
- higher probative value of a qualified signature, vs. a AdES one

Only a thing in the EU

- only true for EU, not a known concept in the US
- but - eIDAS requires *all* digital signatures, including e.g. openpgp ones, to be admissible as proof -> qualified signatures have higher probative value though
- QES signatures
  - only way to replace written contract
  - needs:
    - certified issuer
    - personally identifiable owner (with exclusive access)
    - also needs certified signature device (SSEE - secure signing engine)
      -> then equivalent to hand-written signature

And in Free Software land?

So we want to be able to do secure, digital aDES workflows with Linux!

- using a certified signing device, like Reiner SCT cyberJack RFID

....

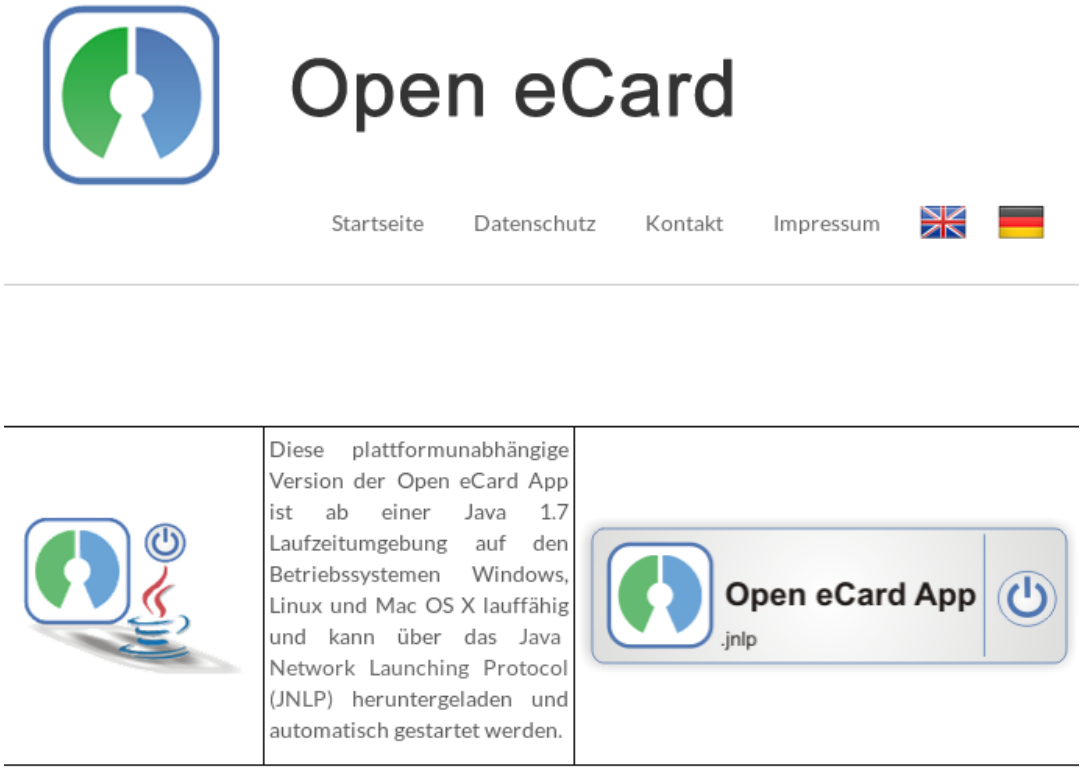
So we want to be able to do secure, digital aDES workflows with Linux!

CIB

- fixed pcsc-cyberjack for openSUSE
  - upstream horror, no real repo, just tarball dumps..
  - unresponsive upstream
  - but there's people patching stuff, e.g.:
  - https://github.com/nunojpg/pcsc-cyberjack.git
    - https://github.com/thorstenb/pcsc-cyberjack.git
    - https://www.openecard.org/download/pc/
  - ugh java .jnlp - https://jnlp.openecard.org/openecard.jnlp
  - but works, eID functions of nPA are available on Linux now
- with that, just load a QES onto your signature card, and stuff works also on linux
- c.f. BeA ...

So we want to be able to do secure, digital aDES workflows with Linux!

- fixed pcsc-cyberjack for openSUSE – nPA stuff now works!
- Use the open eCard .jnlp to interact with service providers



CIB

LibreOffice and OpenPGP

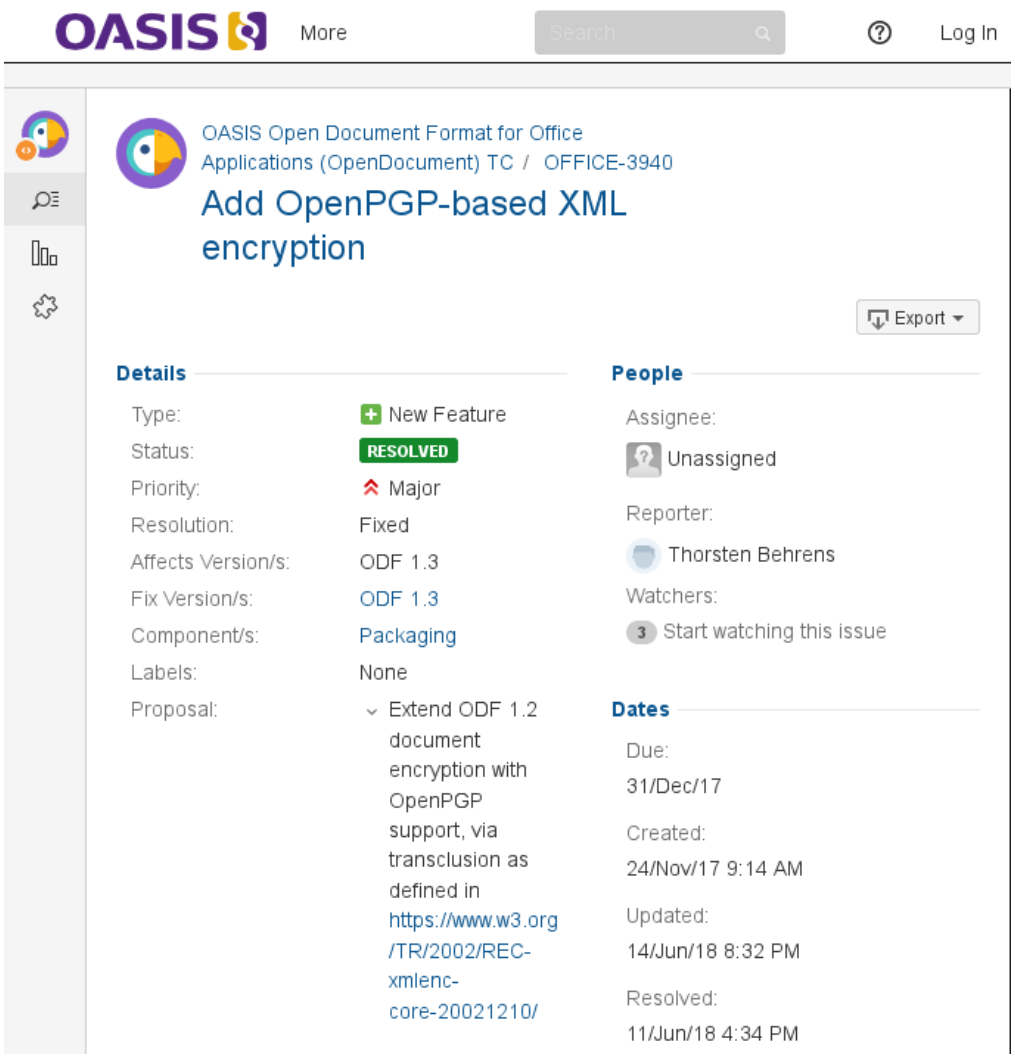
- thanks to BSI, implemented last year, last bits released with LibreOffice 6.0

LibreOffice and OpenPGP

- signing and encryption works since LibreOffice 6.0
- Encryption (with ODF extension namespace) since 6.1
- no time stamps yet -> though this is in theory possible
- GNUPGHOME
- https://issues.oasis-open.org/browse/OFFICE-3940 -> resolved, taken for ODF 1.3
- currently only works for ODF documents
- if you don't see your keys, set GNUPGHOME !

LibreOffice and OpenPGP

- ODF enhancement
  https://issues.oasis-open.org/browse/OFFICE-3940
  -> resolved, taken for ODF 1.3



Gpg4Libre Project

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

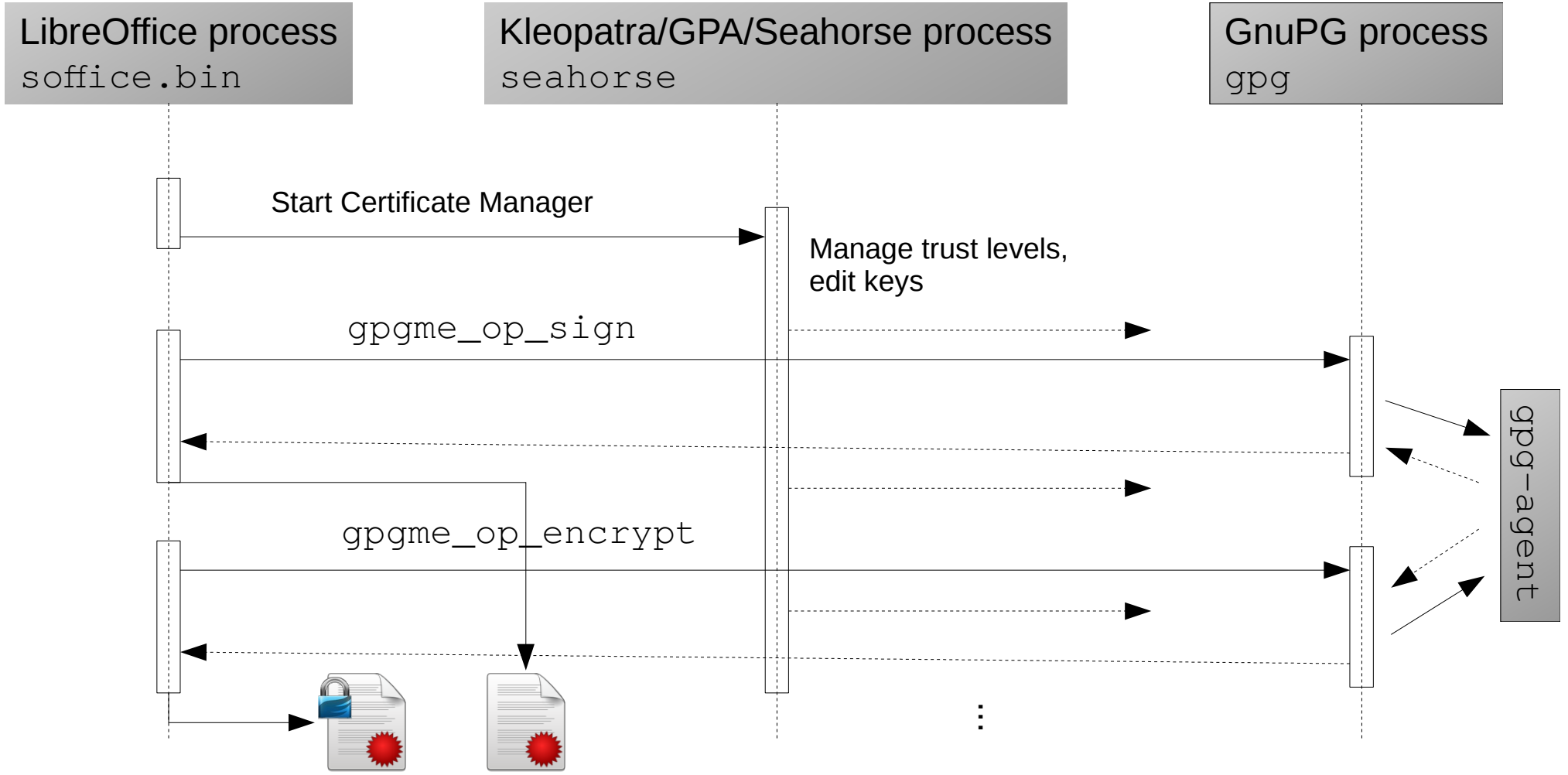
LibreOffice
The Document Foundation

ODF™

SEQUENCE DIAGRAM

Bundesamt für Sicherheit in der Informationstechnik

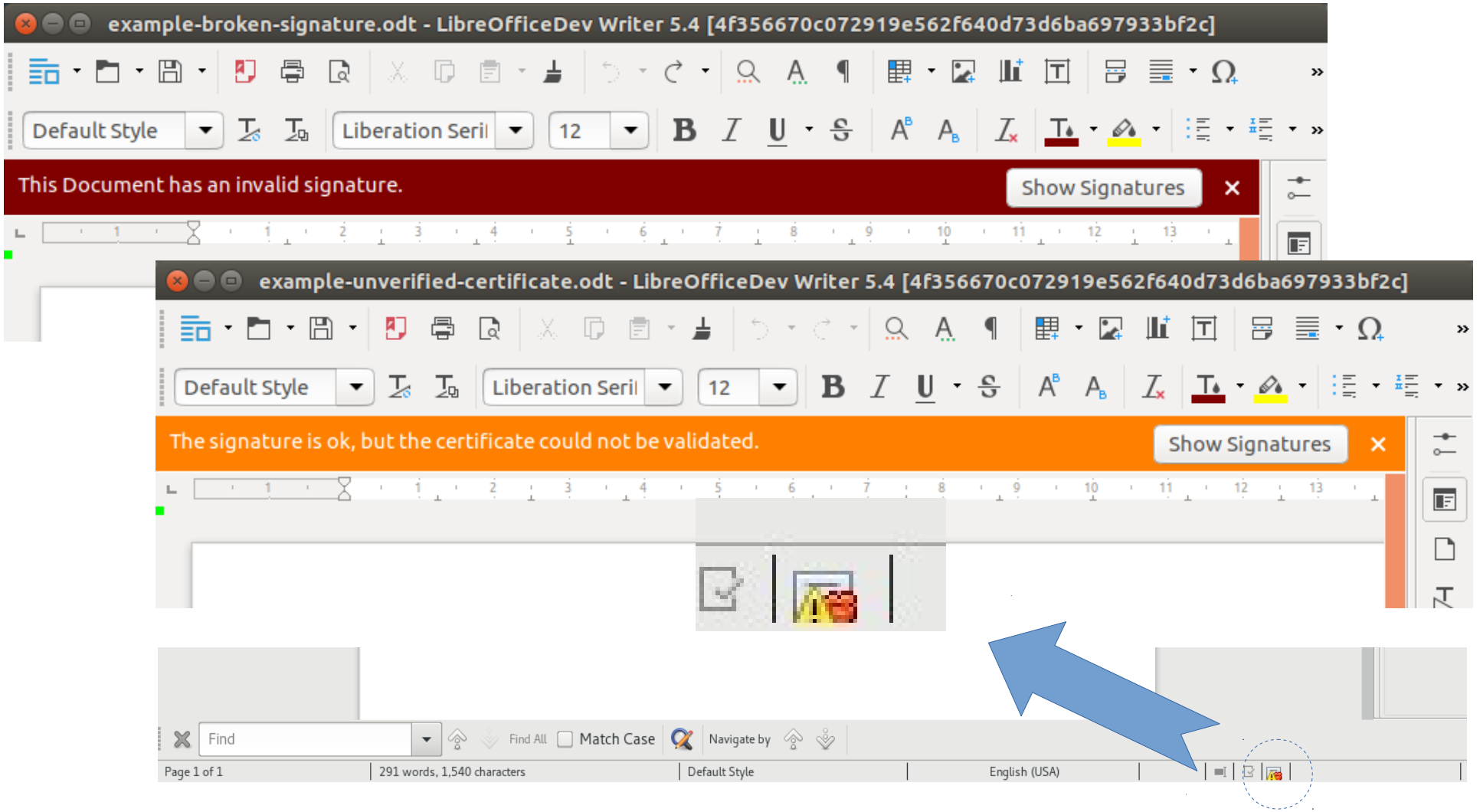
CIB software



UI IMPROVEMENTS

Bundesamt für Sicherheit in der Informationstechnik

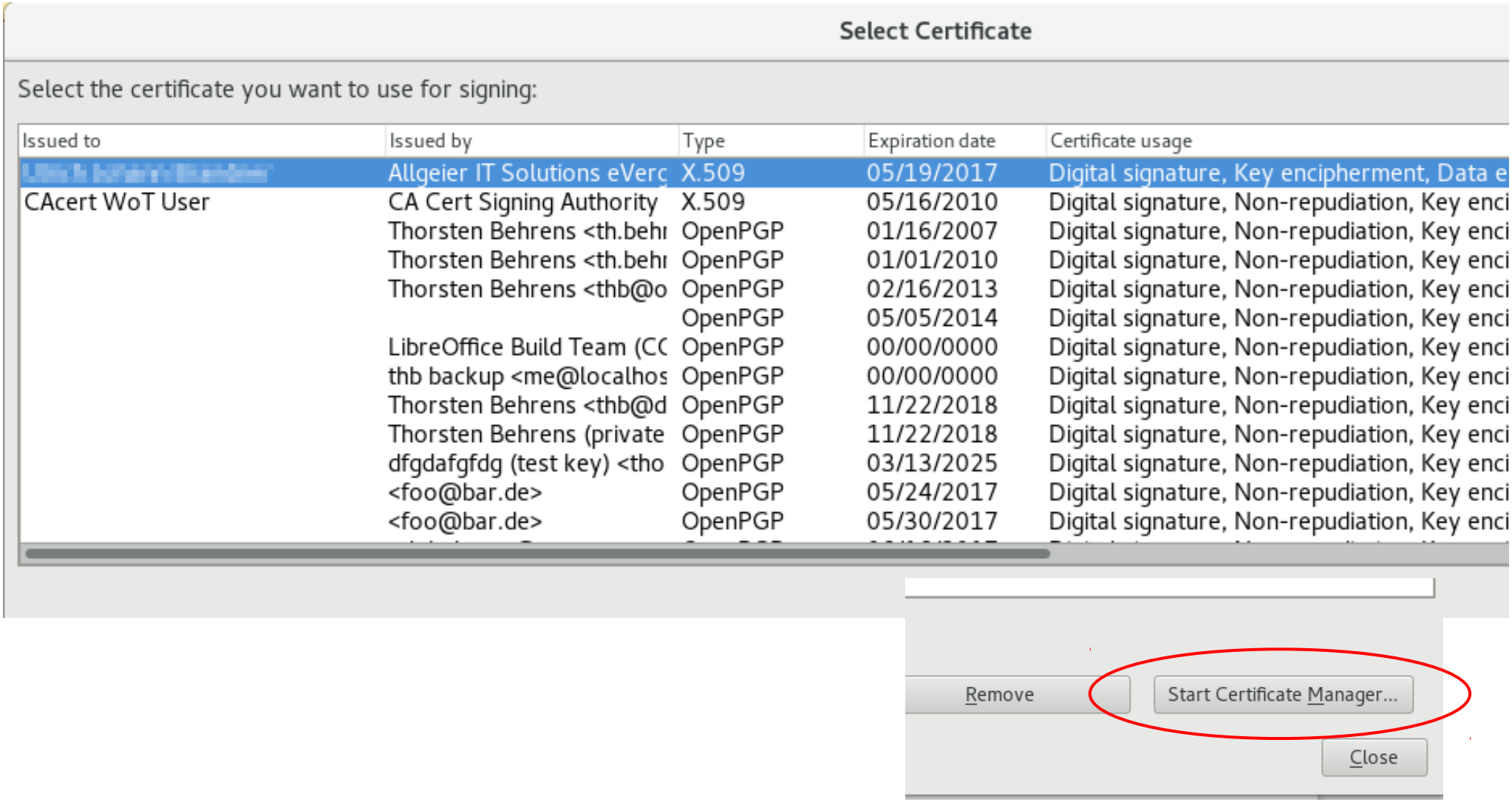
CIB software



INTEGRATING ALL AVAILABLE KEYS

Bundesamt für Sicherheit in der Informationstechnik

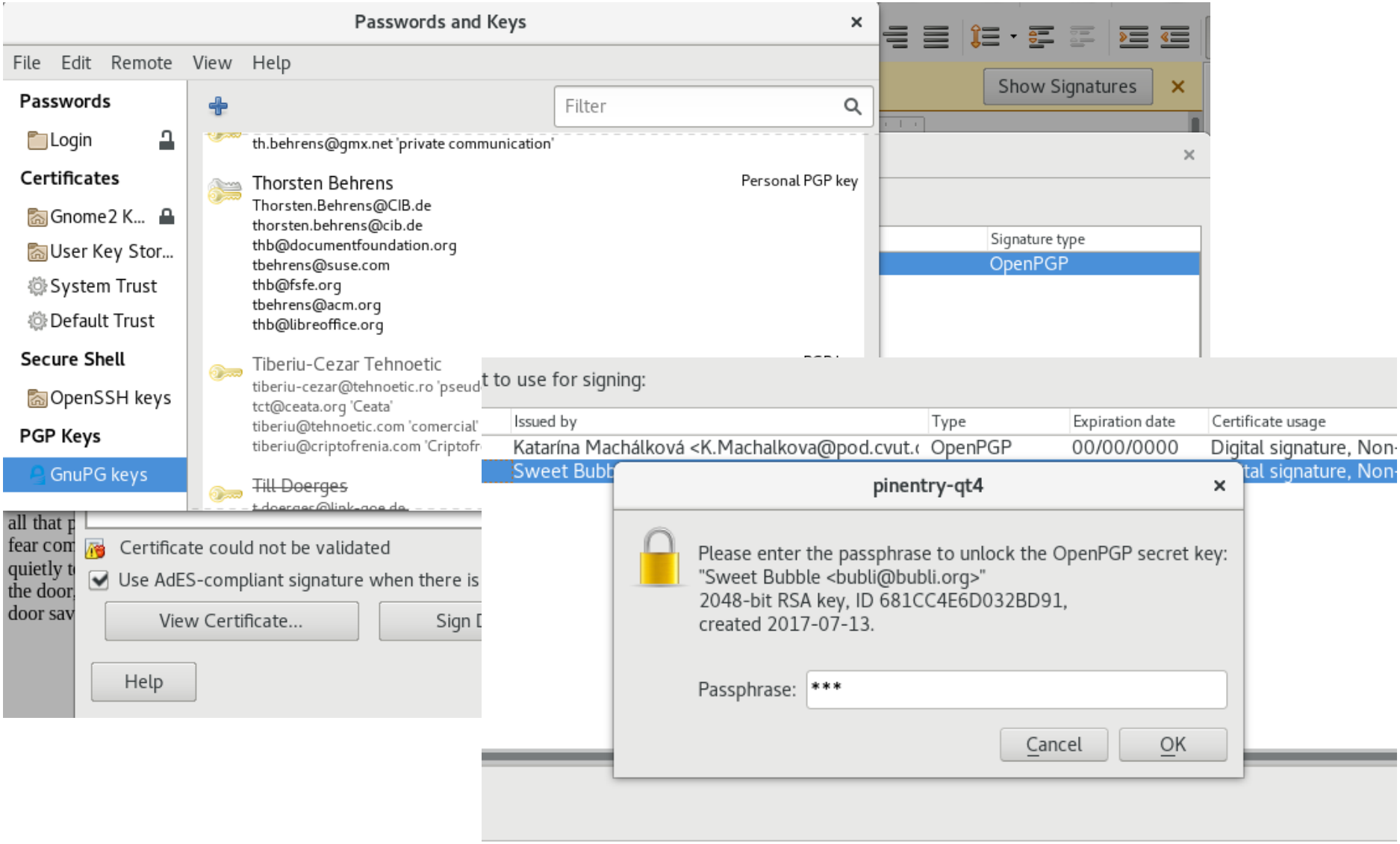
CIB software



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:

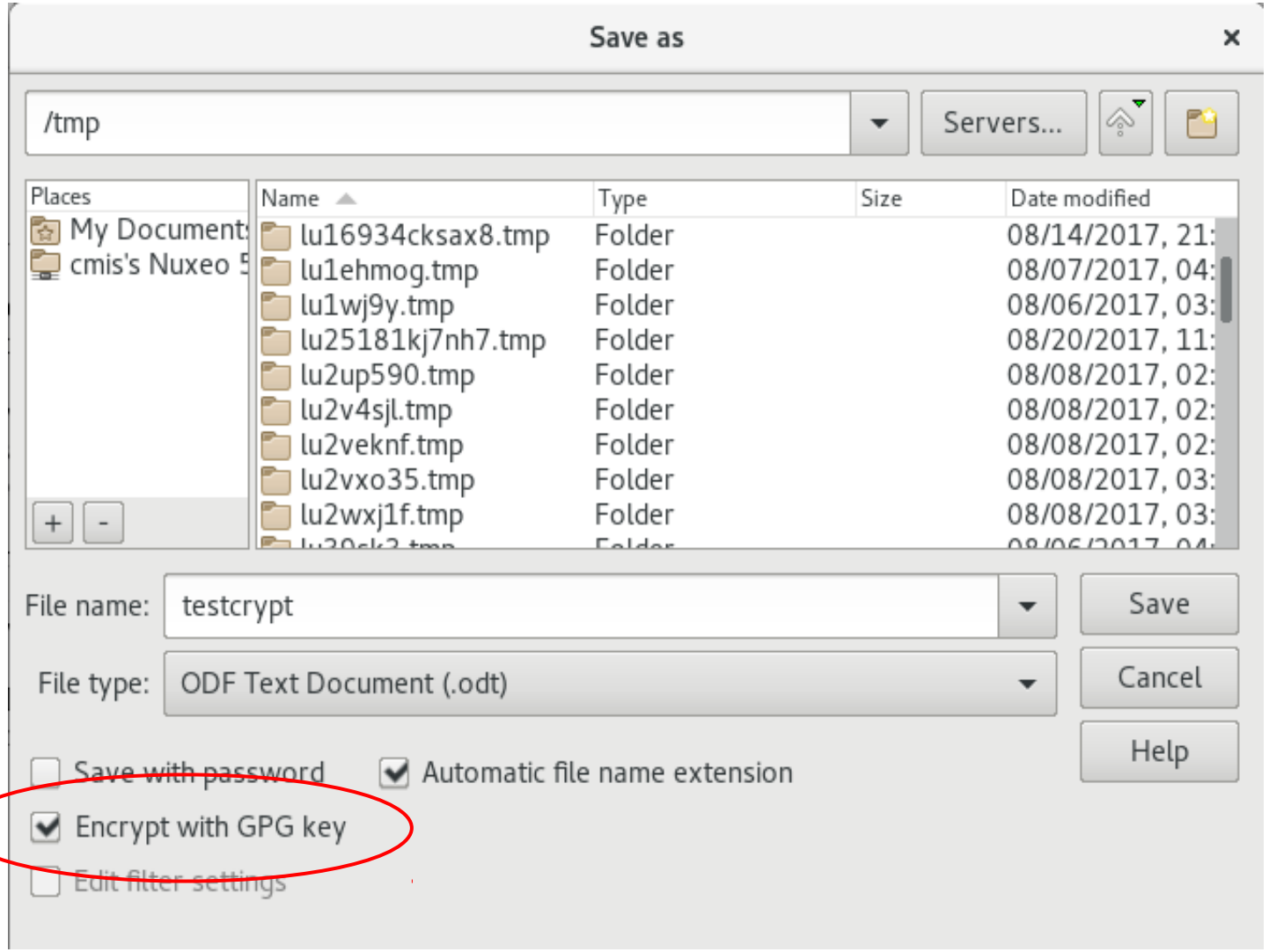
```
<SignatureValue>LS0tLS1CRUdJ...tLS0tCg==</SignatureValue>
<KeyInfo>
  <PGPData>
    <PGPKeyID>OTA5QkUyNTc1Q0VEQkVBMw==</PGPKeyID>
    <PGPKeyPacket>LS0tLS1C...S0tCg==</PGPKeyPacket>
  </PGPData>
</KeyInfo>
```

ENCRYPTION

Bundesamt für Sicherheit in der Informationstechnik

CIB software

- extended save dialog

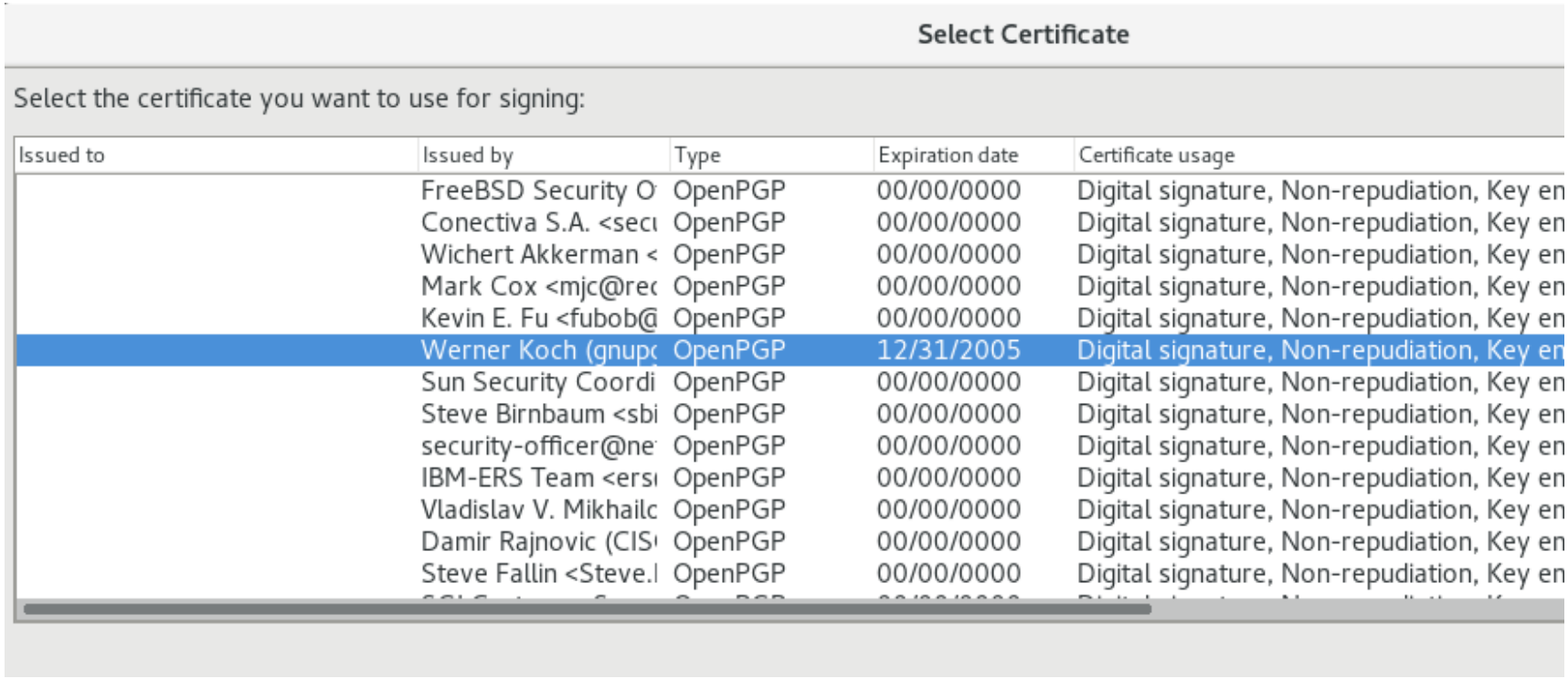


ENCRYPTION

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

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>
```

And X509?

LibreOffice and X509

- available for ODF and OOXML
- available for builtin PDF export
  - most complete for PDF, including timestamps
- if you don't see your certs, set `MOZILLA_CERTIFICATE_FOLDER`

Further workflow / user-facing features

LibreOffice and advanced UI features

- thanks to Limux / City of Munich!
- works for both OOXML and ODF
- available since LibreOffice 6.1
- currently uses some ODF extension
- currently works nicely for X509 signatures

LiMux

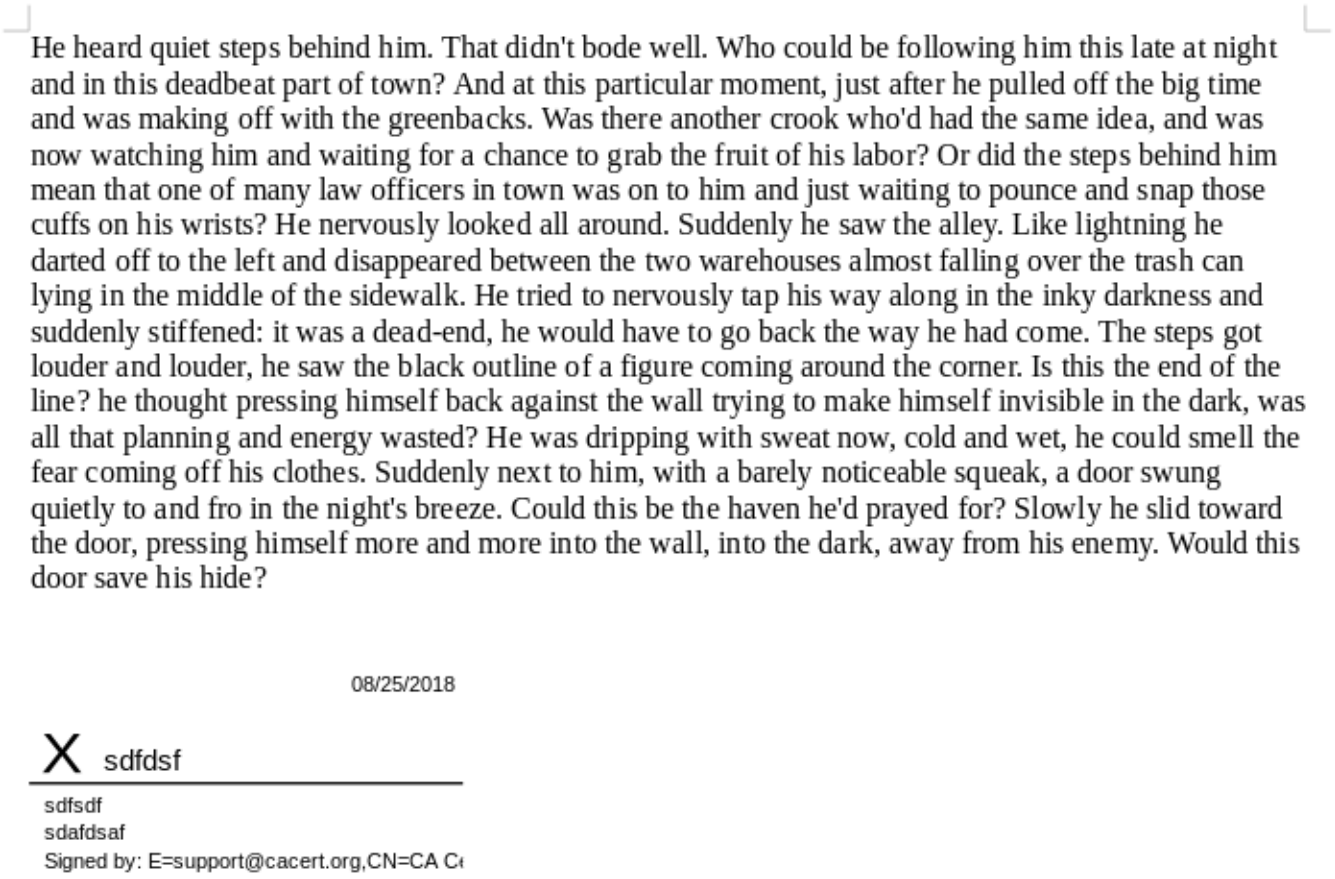
Die IT-Evolution

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 Import & Export
  - Generate new Signature Lines
  - Digitally sign Signature Lines

SIGNATURE LINES

- Visual representation of document signature



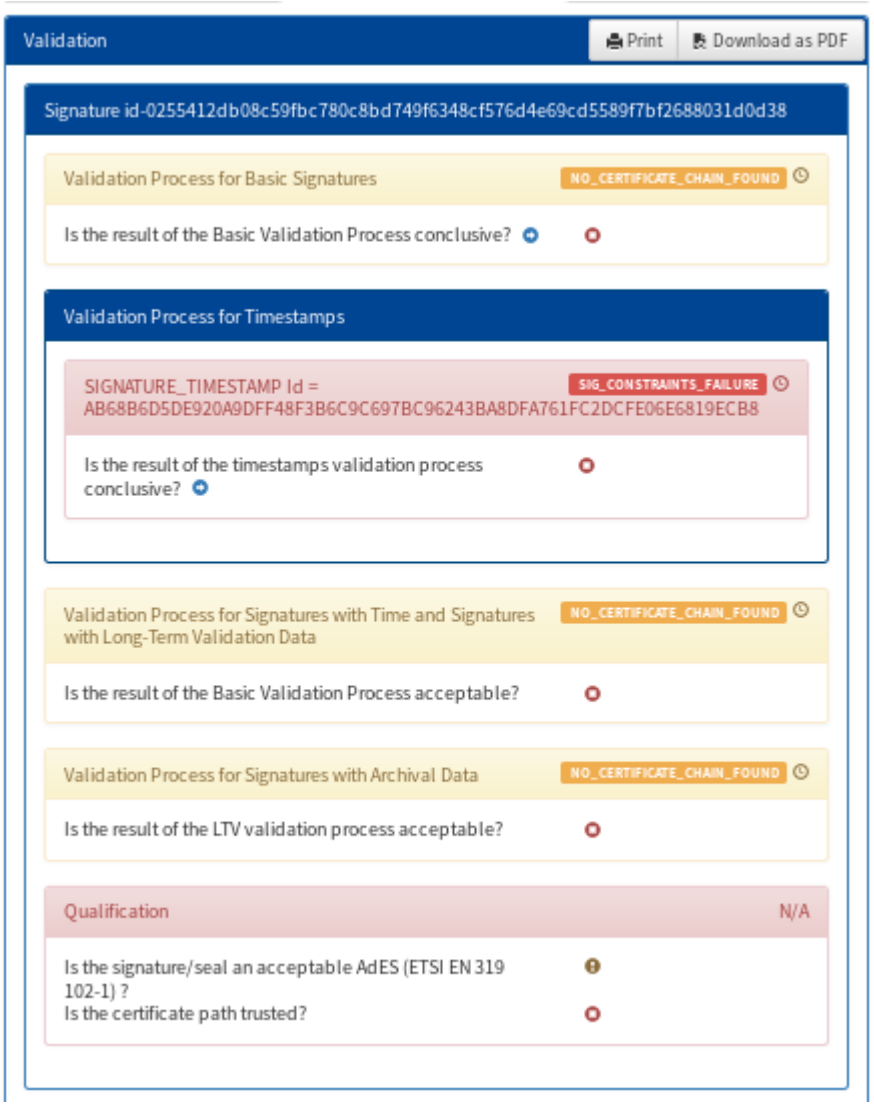
Further userland tools

Support for checking digital signatures

- check digital signatures:
  - For ODF and OOXML, just load the file
  - For PDF, also within LibreOffice – just load the file!
  - or via `$ pdfsig tmp/bug83877SignatureLine.pdf` (part of poppler these days)
  - or via the real deal - official digital signature service DSS EU project:
    - https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature
    - https://github.com/esig/dss.git - LGPL
      - bundle for webservice is there, so you can deploy that internally
    - online demo - validate a signature: https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation
    - also checks the timestamp

Support for checking digital PDF signatures

- online demo - validate a signature: https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation



ROADMAP

- ODF-conformant signing on Linux
  - ships with LibreOffice 5.4
- ODF-conformant signing also on Windows
  - shipped for LibreOffice 6.0 (Feb. 2018)
  - Works also for OS X – open for Android
- experimental encryption on Linux & Windows
  - shipping for LibreOffice 6.0 (Feb. 2018)
  - with ODF extension namespace
- ODF 1.3
  - proposed XMLSEC-extensions for OpenPGP encryption to OASIS ODF TC – GA for 1.3 around 2019
- Further signature line improvements in 6.2, reading and writing standard-conformant ODF 1.3 encryption – due February 2019

THANK YOU!

OUR PRODUCTS:

HTTP://LIBREOFFICE.CIB.DE/

WE CAN HELP:

HTTP://LIBREOFFICE.CIB.DE/SUPPORT