

---

# DIGITAL SIGNATURE AND ENCRYPTION WORKFLOWS WITH LIBREOFFICE

FrOSCon 2018

[Thorsten.Behrens@cib.de](mailto:Thorsten.Behrens@cib.de)



Bundesamt  
für Sicherheit in der  
Informationstechnik

# Who am I?

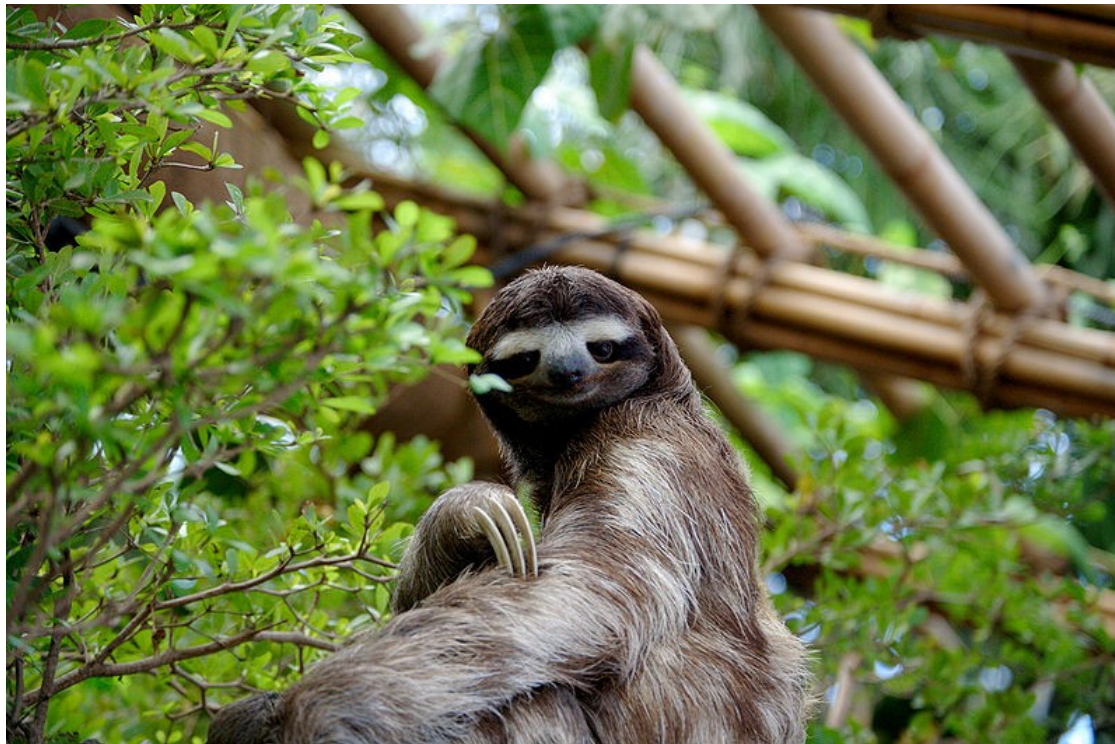
## Thorsten Behrens

- 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](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

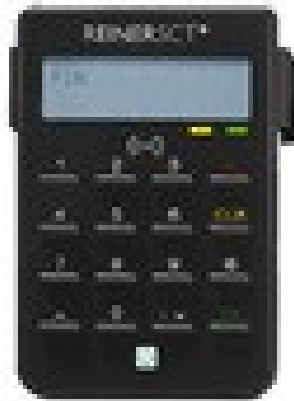
- only true for EU, not a known concept in the US
  - but - eIDAS requires *all* digital signatures, including e.g. openpgp ones, to be admissible as proof -> qualified signatures have higher probative value though
  - QES signatures
    - only way to replace written contract
    - needs:
      - certified 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!

- 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



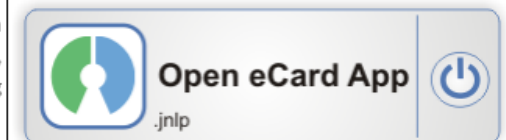
## Open eCard

[Startseite](#)
[Datenschutz](#)
[Kontakt](#)
[Impressum](#)





Diese plattformunabhängige Version der Open eCard App ist ab einer Java 1.7 Laufzeitumgebung auf den Betriebssystemen Windows, Linux und Mac OS X lauffähig und kann über das Java Network Launching Protocol (JNLP) heruntergeladen und automatisch gestartet werden.



# LibreOffice and OpenPGP

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



Bundesamt  
für Sicherheit in der  
Informationstechnik



# LibreOffice and OpenPGP

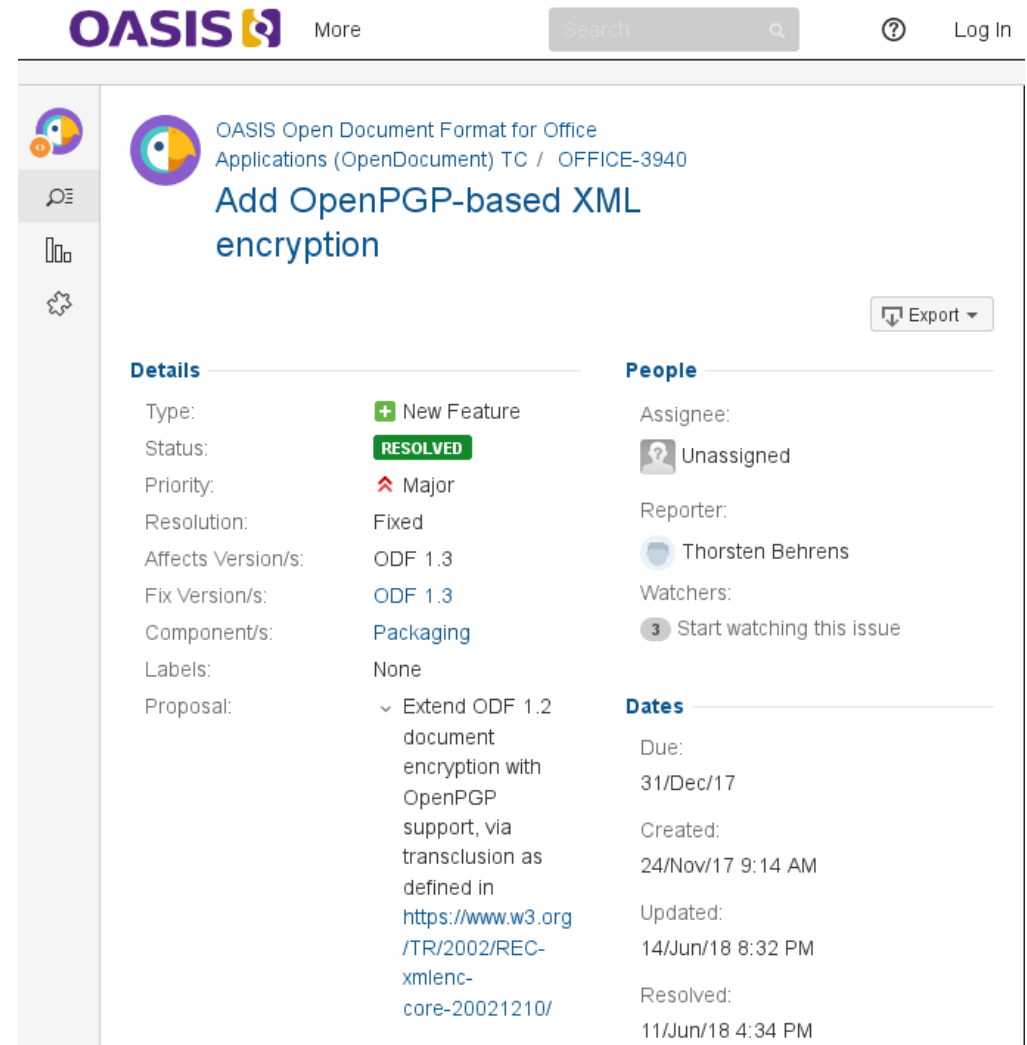
- signing and encryption works since LibreOffice 6.0
  - Encryption (with ODF extension namespace) since 6.1
  - no time stamps yet -> though this is in theory possible
  - GNUPGHOME
  - <https://issues.oasis-open.org/browse/OFFICE-3940> -> resolved, taken for ODF 1.3
  - currently only works for ODF 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



**OASIS** More  ? Log In

**OASIS Open Document Format for Office Applications (OpenDocument) TC / OFFICE-3940**

## Add OpenPGP-based XML encryption

[Export](#)

**Details**

Type: + New Feature  
 Status: RESOLVED  
 Priority: ^ Major  
 Resolution: Fixed  
 Affects Version/s: ODF 1.3  
 Fix Version/s: ODF 1.3  
 Component/s: Packaging  
 Labels: None  
 Proposal: v Extend ODF 1.2 document encryption with OpenPGP support, via transclusion as defined in <https://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>

**People**

Assignee: Unassigned  
 Reporter: Thorsten Behrens  
 Watchers: 3 Start watching this issue

**Dates**

Due: 31/Dec/17  
 Created: 24/Nov/17 9:14 AM  
 Updated: 14/Jun/18 8:32 PM  
 Resolved: 11/Jun/18 4:34 PM

# Gpg4Libre Project



# 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



⋮



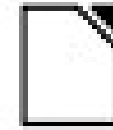
Seahorse

⋮

IPC / execute



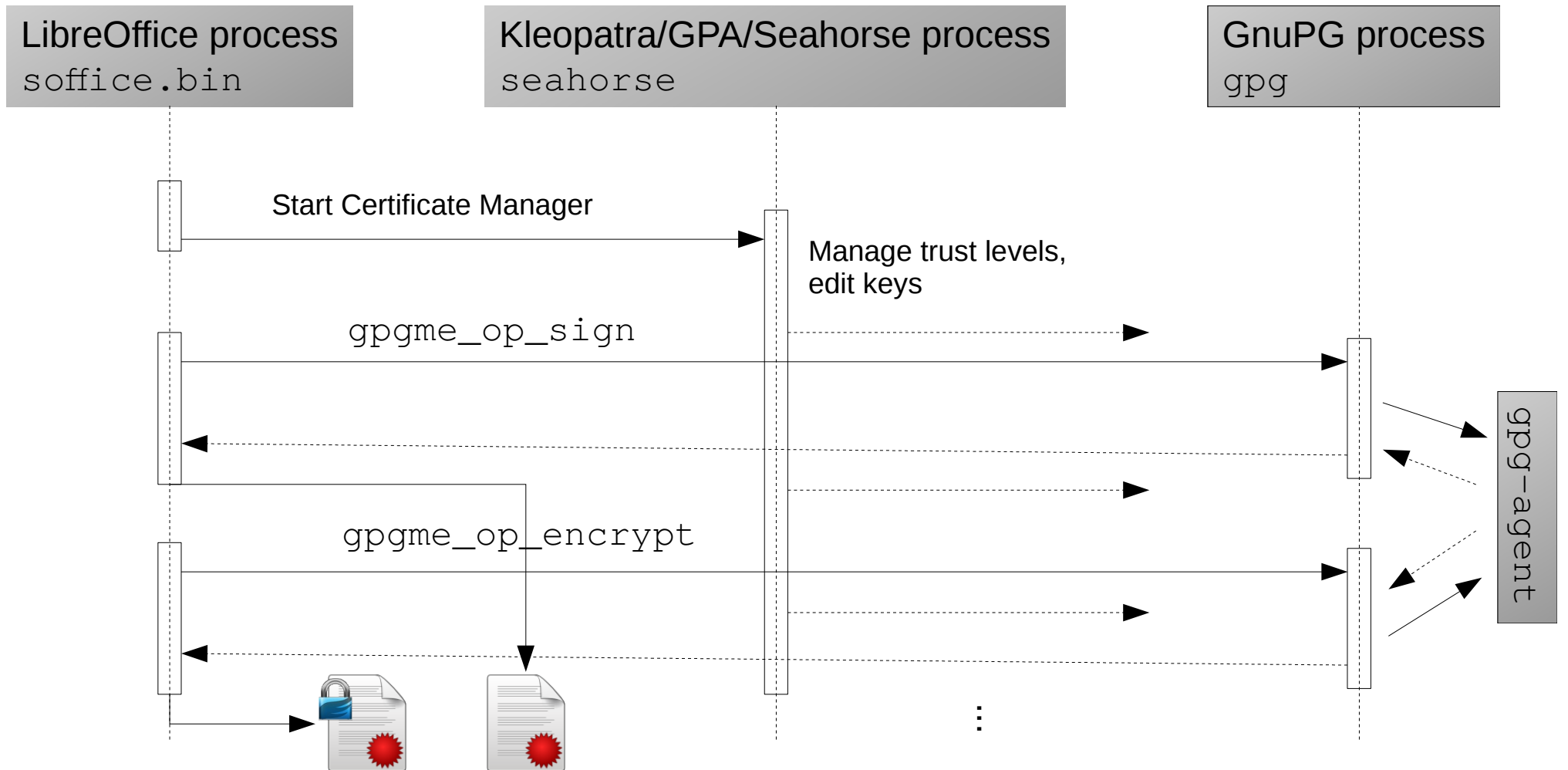
gpgme



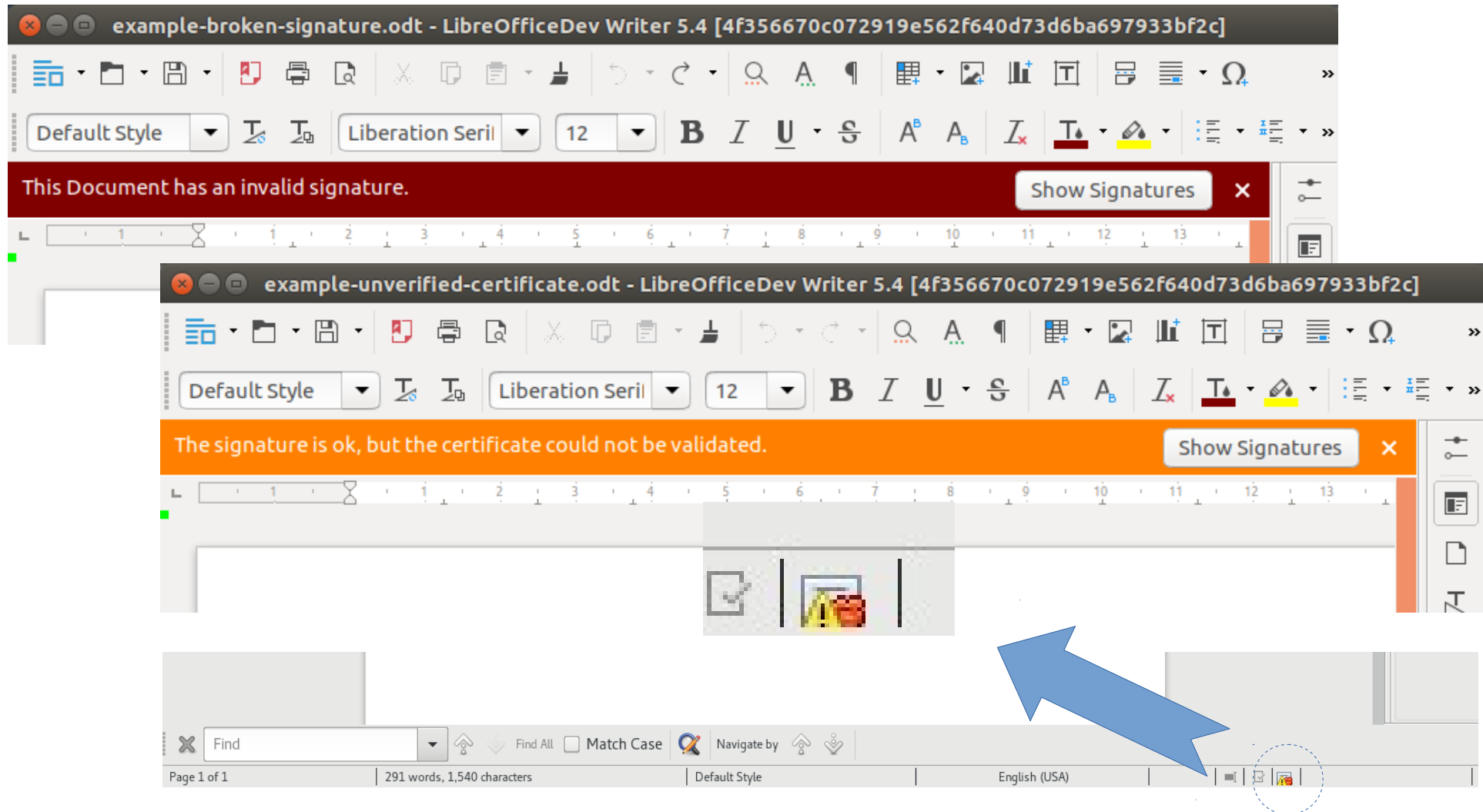
**LibreOffice**  
The Document Foundation



# 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 (C...	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



# 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>
```

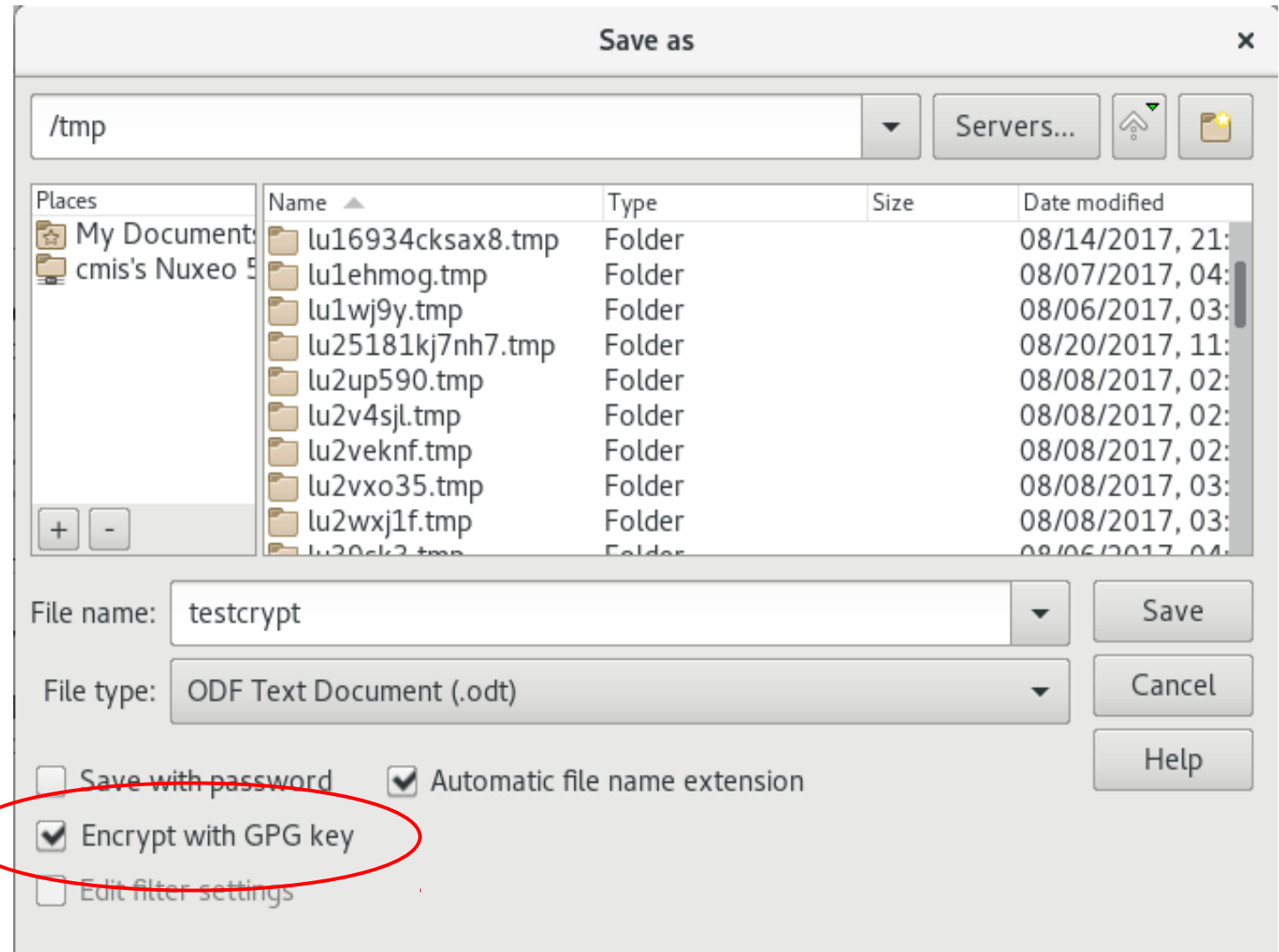
---



# 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

# 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>
```

---

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

He heard quiet steps behind him. That didn't bode well. Who could be following him this late at night and in this deadbeat part of town? And at this particular moment, just after he pulled off the big time and was making off with the greenbacks. Was there another crook who'd had the same idea, and was now watching him and waiting for a chance to grab the fruit of his labor? Or did the steps behind him mean that one of many law officers in town was on to him and just waiting to pounce and snap those cuffs on his wrists? He nervously looked all around. Suddenly he saw the alley. Like lightning he darted off to the left and disappeared between the two warehouses almost falling over the trash can lying in the middle of the sidewalk. He tried to nervously tap his way along in the inky darkness and suddenly stiffened: it was a dead-end, he would have to go back the way he had come. The steps got louder and louder, he saw the black outline of a figure coming around the corner. Is this the end of the line? he thought pressing himself back against the wall trying to make himself invisible in the dark, was all that planning and energy wasted? He was dripping with sweat now, cold and wet, he could smell the fear coming off his clothes. Suddenly next to him, with a barely noticeable squeak, a door swung quietly to and fro in the night's breeze. Could this be the haven he'd prayed for? Slowly he slid toward the door, pressing himself more and more into the wall, into the dark, away from his enemy. Would this door save his hide?

08/25/2018

X sdfdsf

sdfsdf

sdafdsaf

Signed by: E=support@cacert.org,CN=CA C

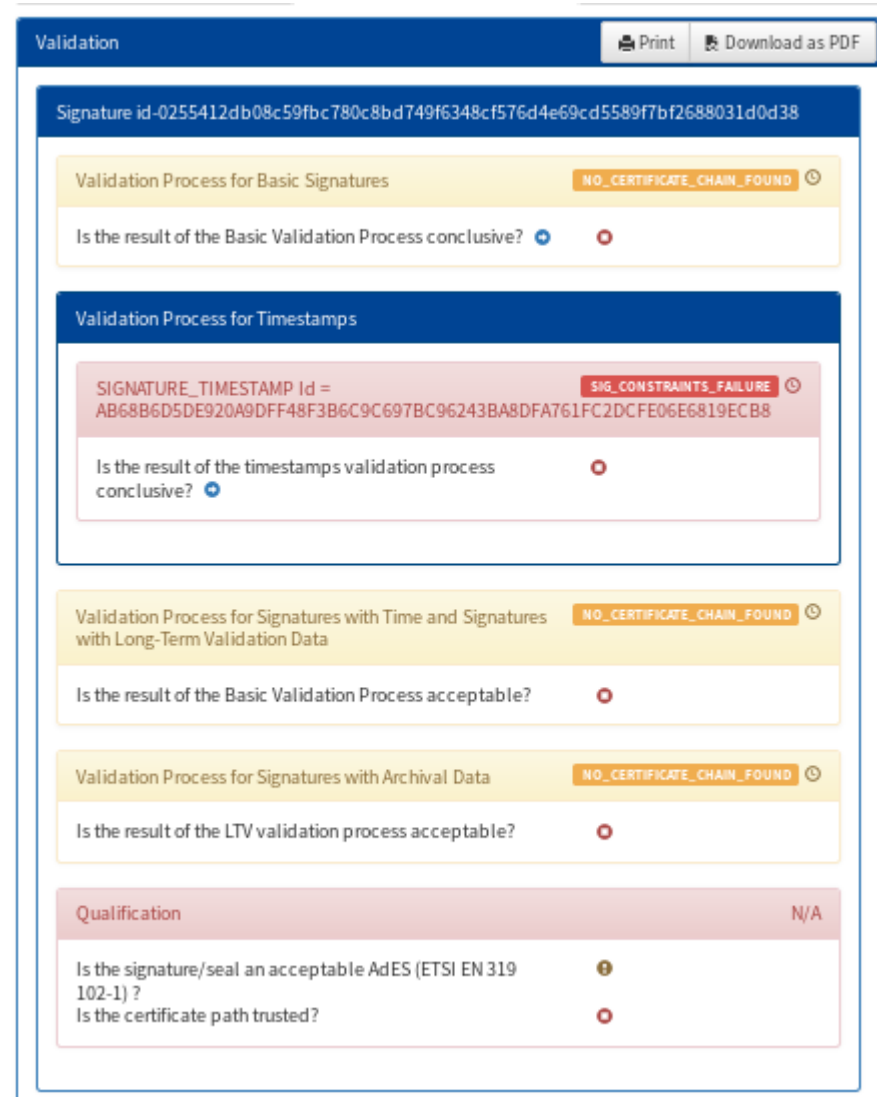
Further userland tools

# 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>



The screenshot shows a web application interface for validating digital signatures. The page title is "Validation" and it includes "Print" and "Download as PDF" buttons. The main content area displays the following information:

- Signature id:** id-0255412db08c59fbc780c8bd749f6348cf576d4e69cd5589f7bf2688031d0d38
- Validation Process for Basic Signatures:**
  - Status: NO\_CERTIFICATE\_CHAIN\_FOUND
  - Is the result of the Basic Validation Process conclusive?
- Validation Process for Timestamps:**
  - SIGNATURE\_TIMESTAMP Id = AB68B6D5DE920A9DFF48F3B6C9C697BC96243BA8DFA761FC2DCFE06E6819ECB8
  - Status: SIG\_CONSTRAINTS\_FAILURE
  - Is the result of the timestamps validation process conclusive?
- Validation Process for Signatures with Time and Signatures with Long-Term Validation Data:**
  - Status: NO\_CERTIFICATE\_CHAIN\_FOUND
  - Is the result of the Basic Validation Process acceptable?
- Validation Process for Signatures with Archival Data:**
  - Status: NO\_CERTIFICATE\_CHAIN\_FOUND
  - Is the result of the LTV validation process acceptable?
- Qualification:**
  - Status: N/A
  - Is the signature/seal an acceptable AdES (ETSI EN 319 102-1)?
  - Is the certificate path trusted?

# 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/](http://libreoffice.cib.de/)**

**WE CAN HELP:**

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

