OpenPGP.conf Sept 8th 2016

Aiming for: many more OpenPGP Email users 2017

Bernhard E. Reiter


GPG
4WiN


GPG
4WiN

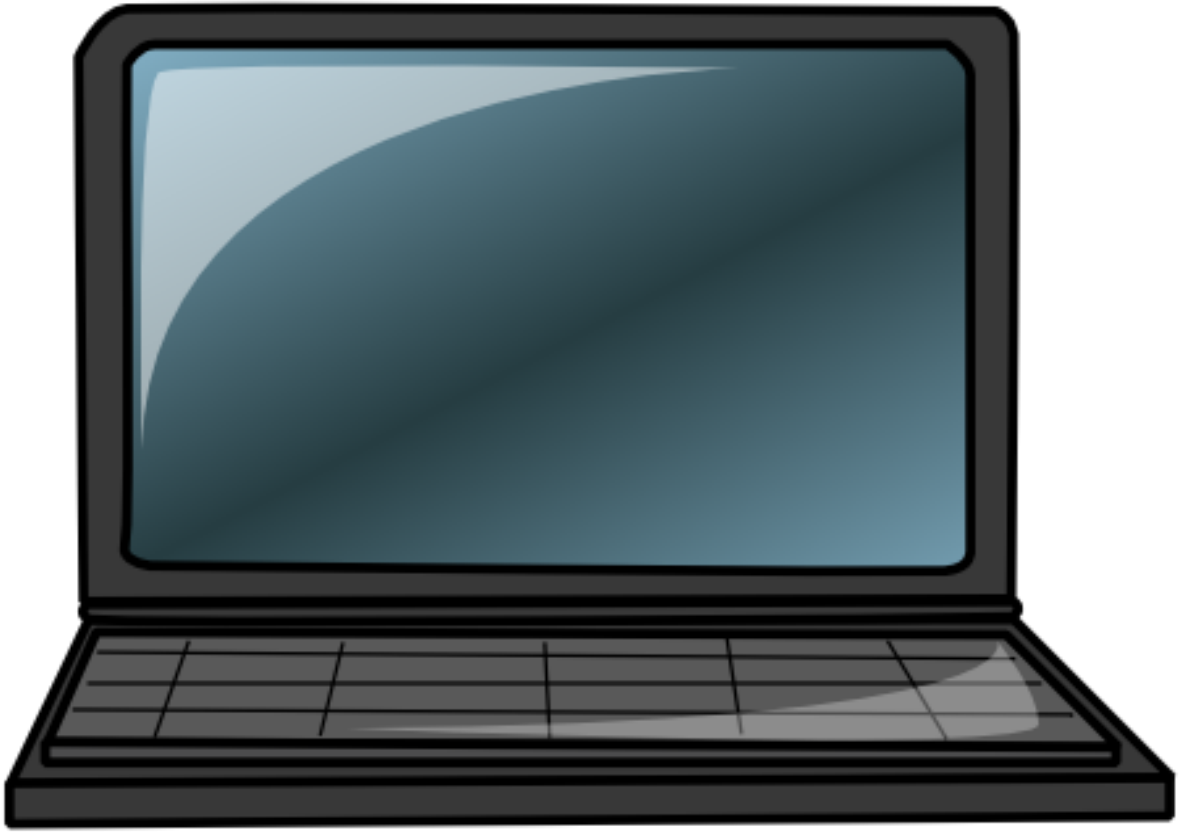
User experience (no need to manage “trust”)

Ideas for:

- Android
- Web

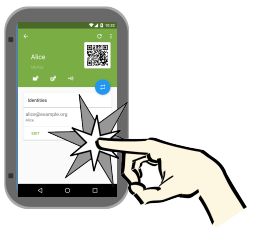
MIME + Exchange with Outlook

“restricted” documents

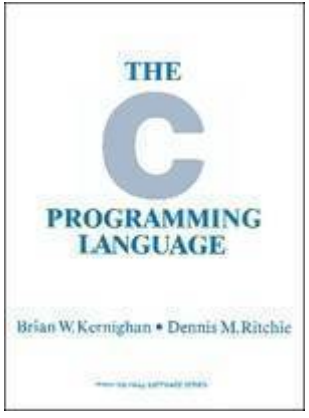


10x

>

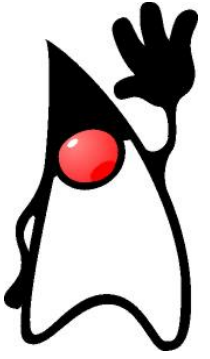


vs

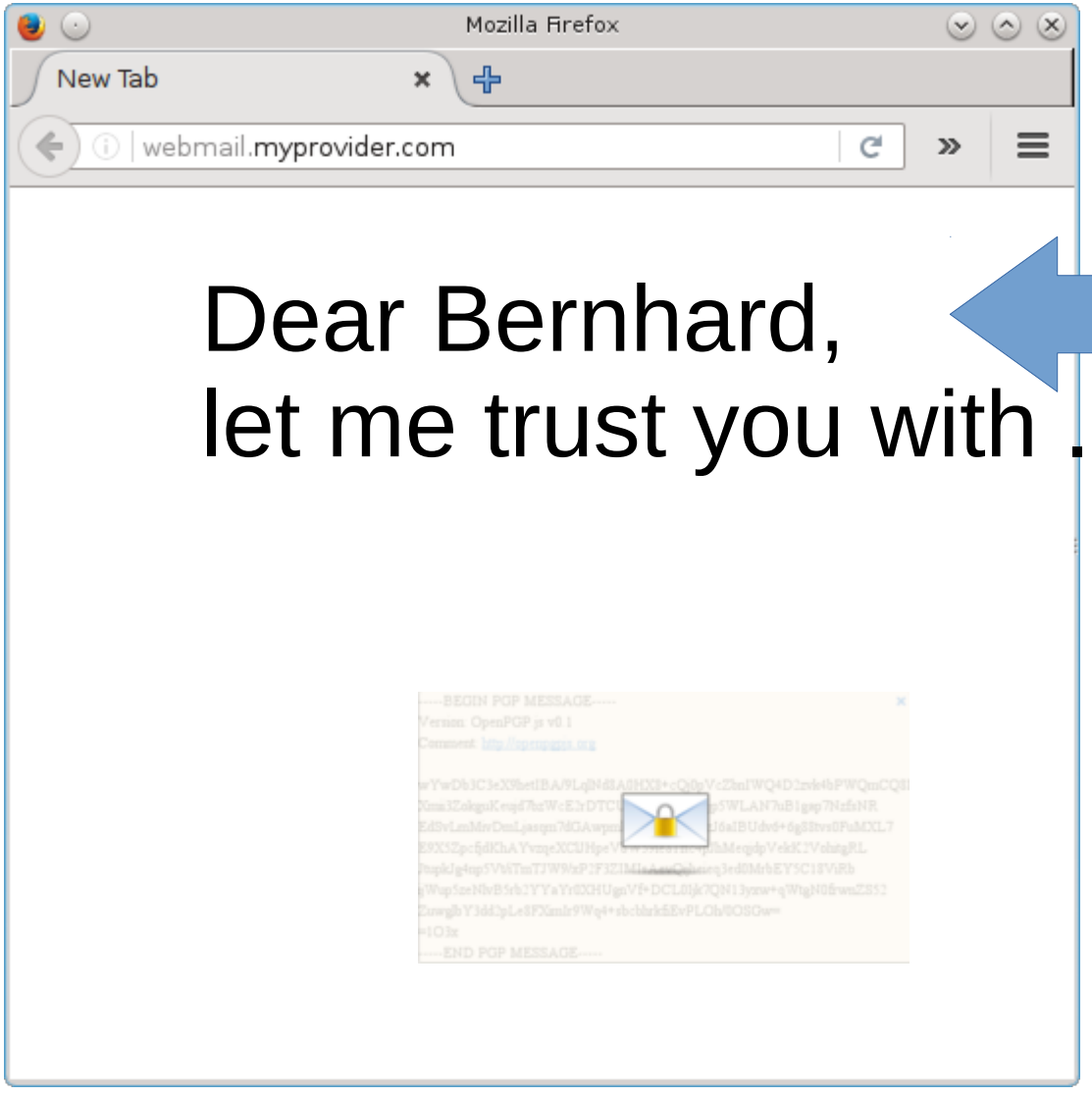


libgcrypt

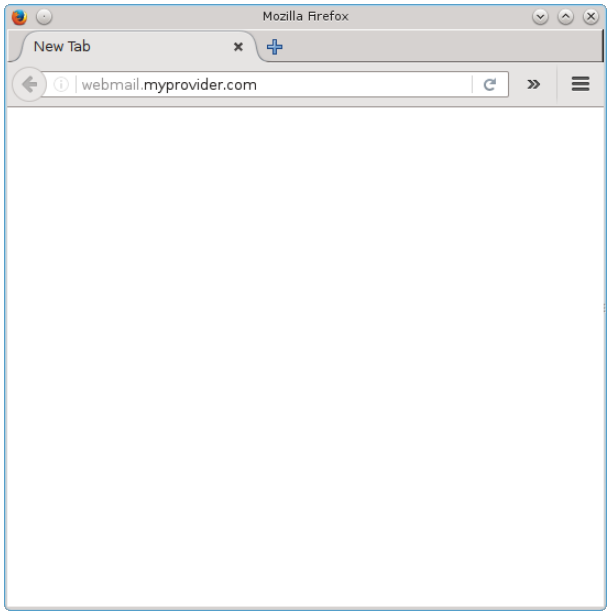
Bouncy Castle

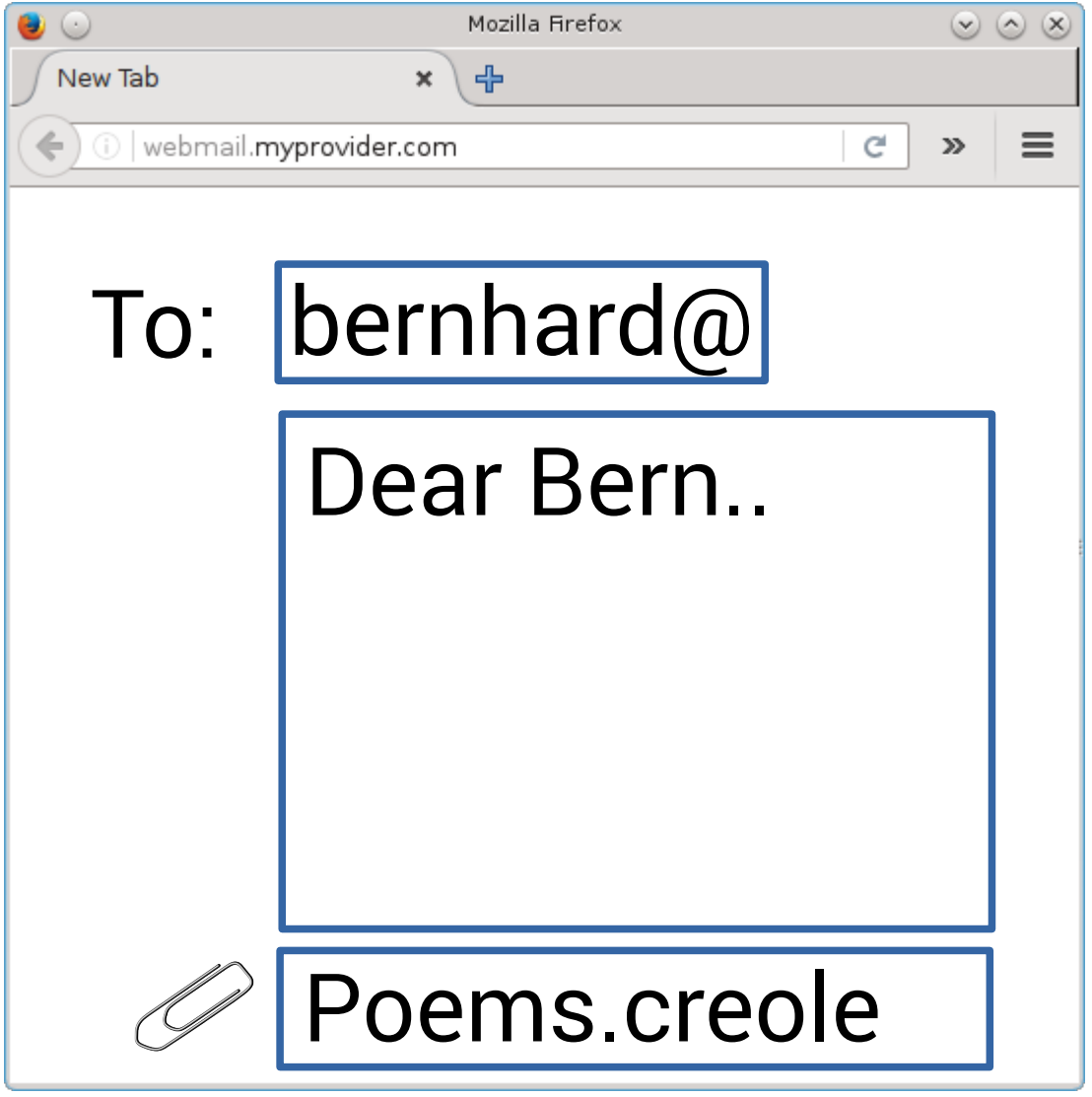


Beware of

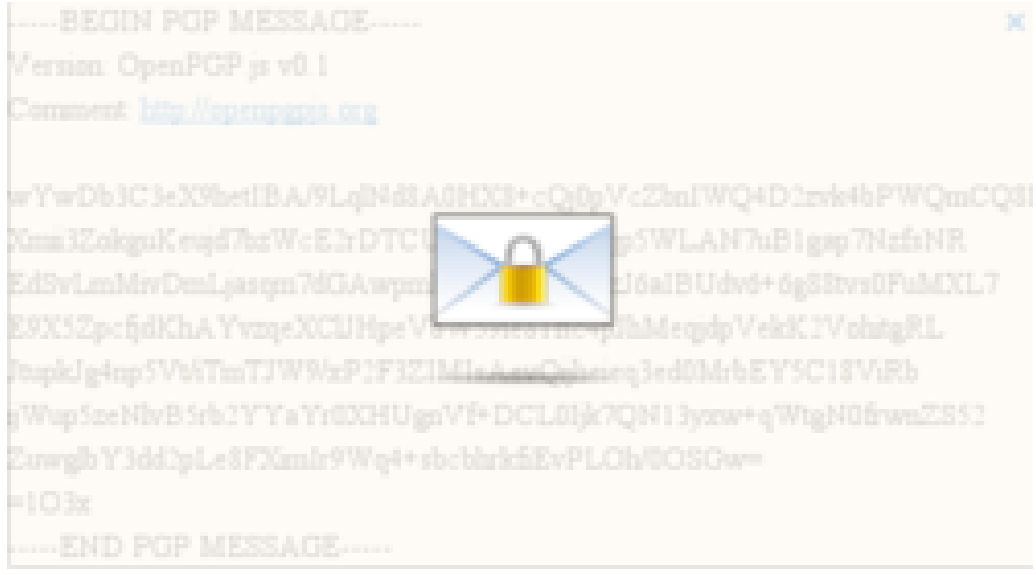

Mozilla Firefox
New Tab
webmail.myprovider.com
Dear Bernhard,
let me trust you with ...

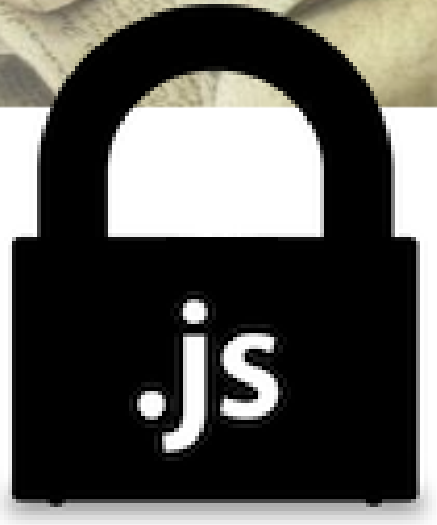

Mozilla Firefox
New Tab
webmail.myprovider.com
.js
WebExtensions


Mozilla Firefox
New Tab
webmail.myprovider.com
Native Messaging


Mozilla Firefox
New Tab
webmail.myprovider.com
To:
bernhard@
Dear Bern..
Poems.creole

Mailvelope





OpenPGP.js

Bundesamt
für Sicherheit in der
Informationstechnik

Public tenders

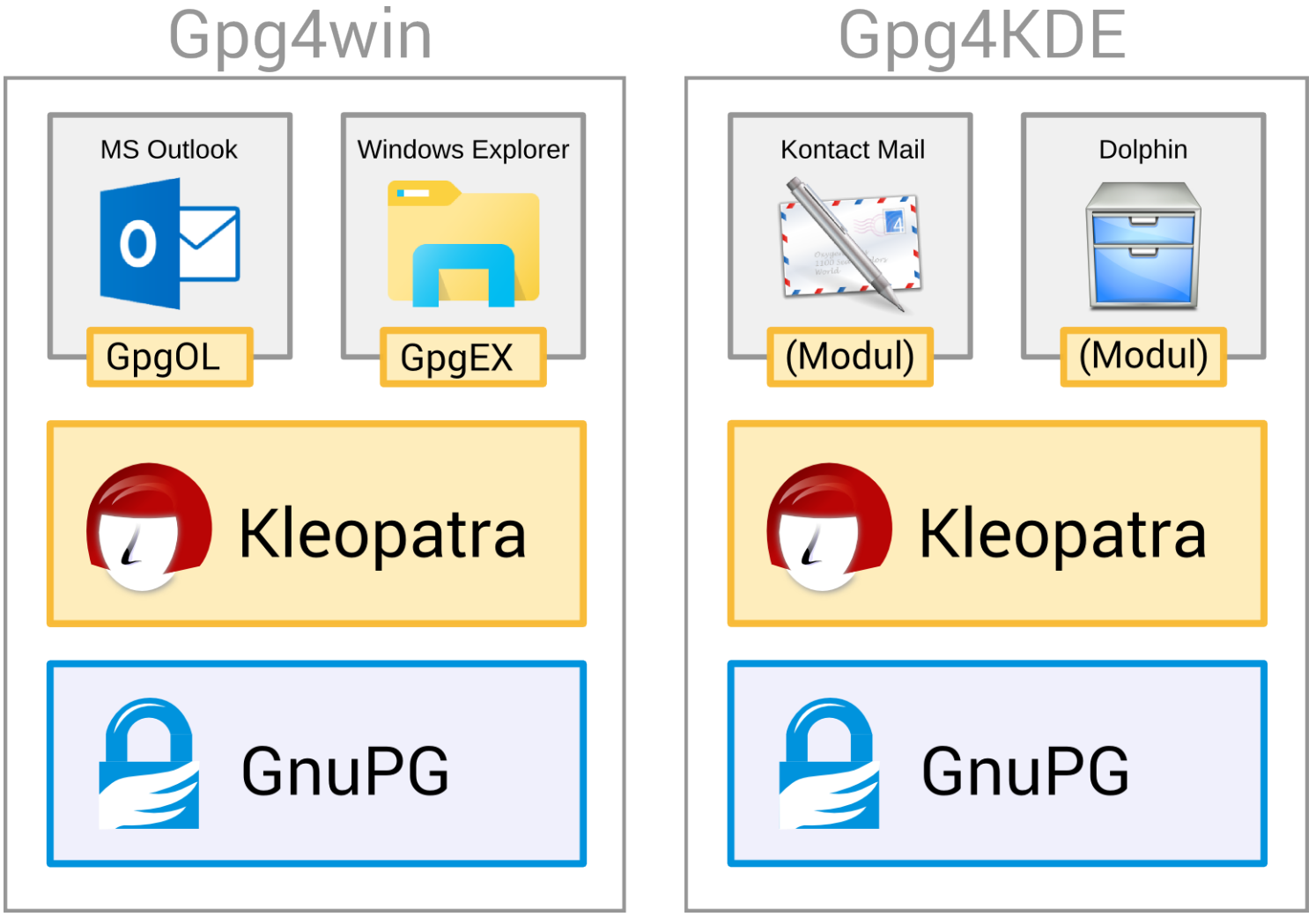
- Emanuel Schütze
- Bernhard Reiter
- Andre Heinecke
- Jochen Saalfeld
- Werner Koch
- Justus Winter
- [..]

Subcontractors

- Thomas Oberndörfer (Mailvelope GmbH)
- Dominik Schürmann (TU Braunschweig, OpenKeychain)
- Vincent Breitmoser (OpenKeychain)
- Oskar Hahn
- KDAB (Deutschland) GmbH & Co. KG
- atsec information security GmbH

Public

- ML
- Wiki
- Code
- Free Software

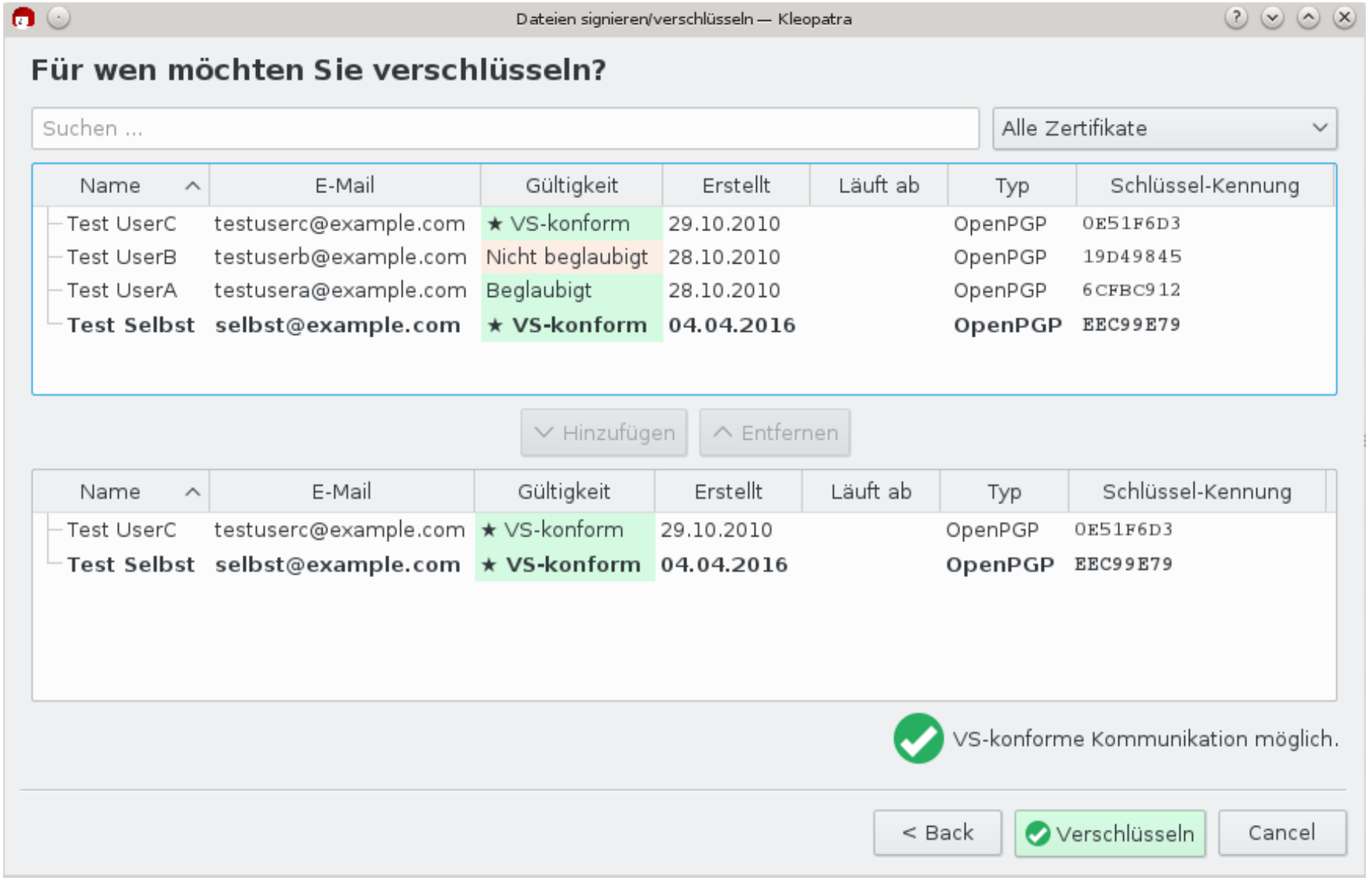

Gpg4win
MS Outlook
GpgOL
Windows Explorer
GpgEX
Kleopatra
GnuPG
Gpg4KDE
Kontact Mail
(Modul)
Dolphin
(Modul)
Kleopatra
GnuPG

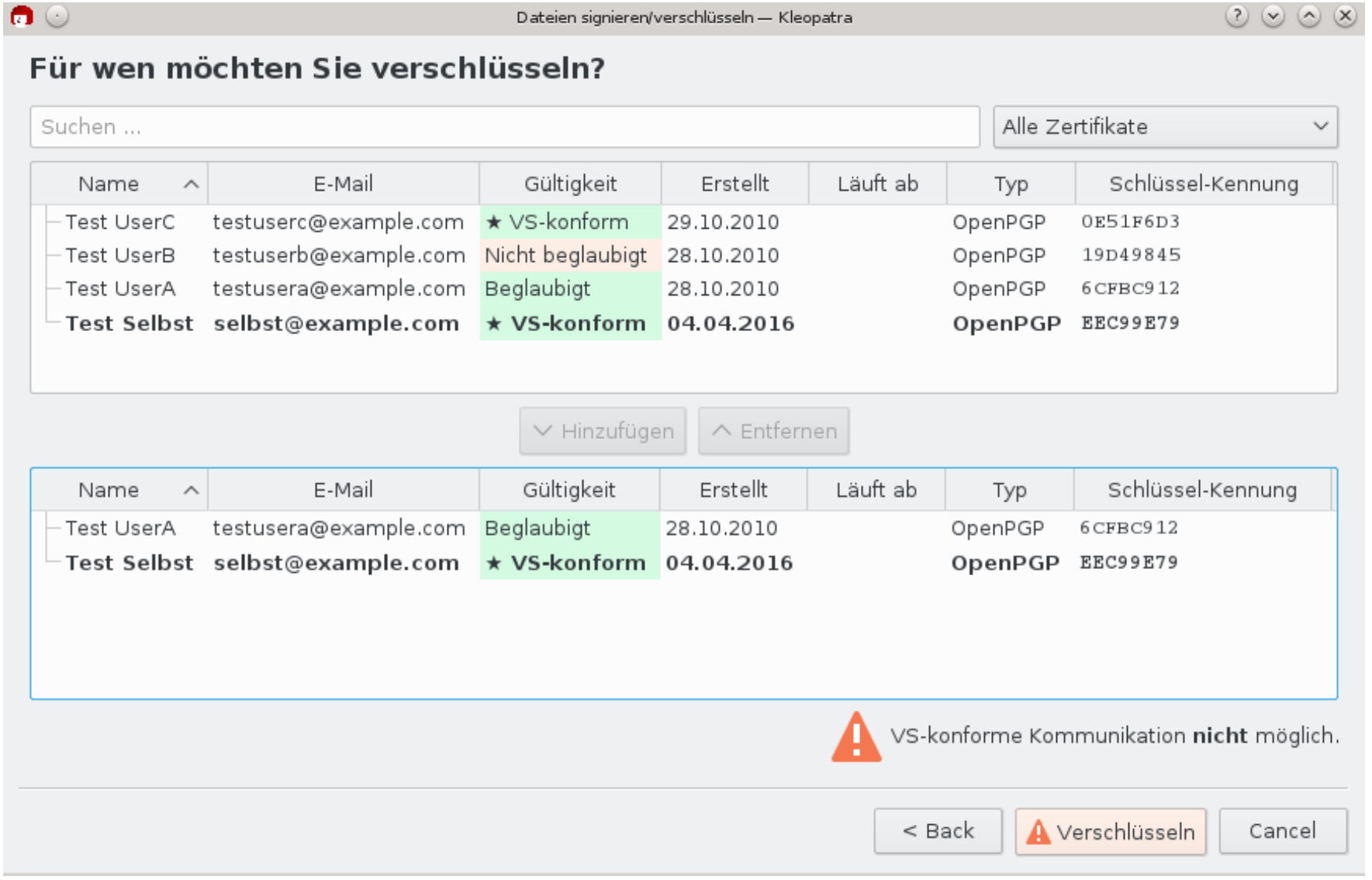
Evaluation → “Checklist“

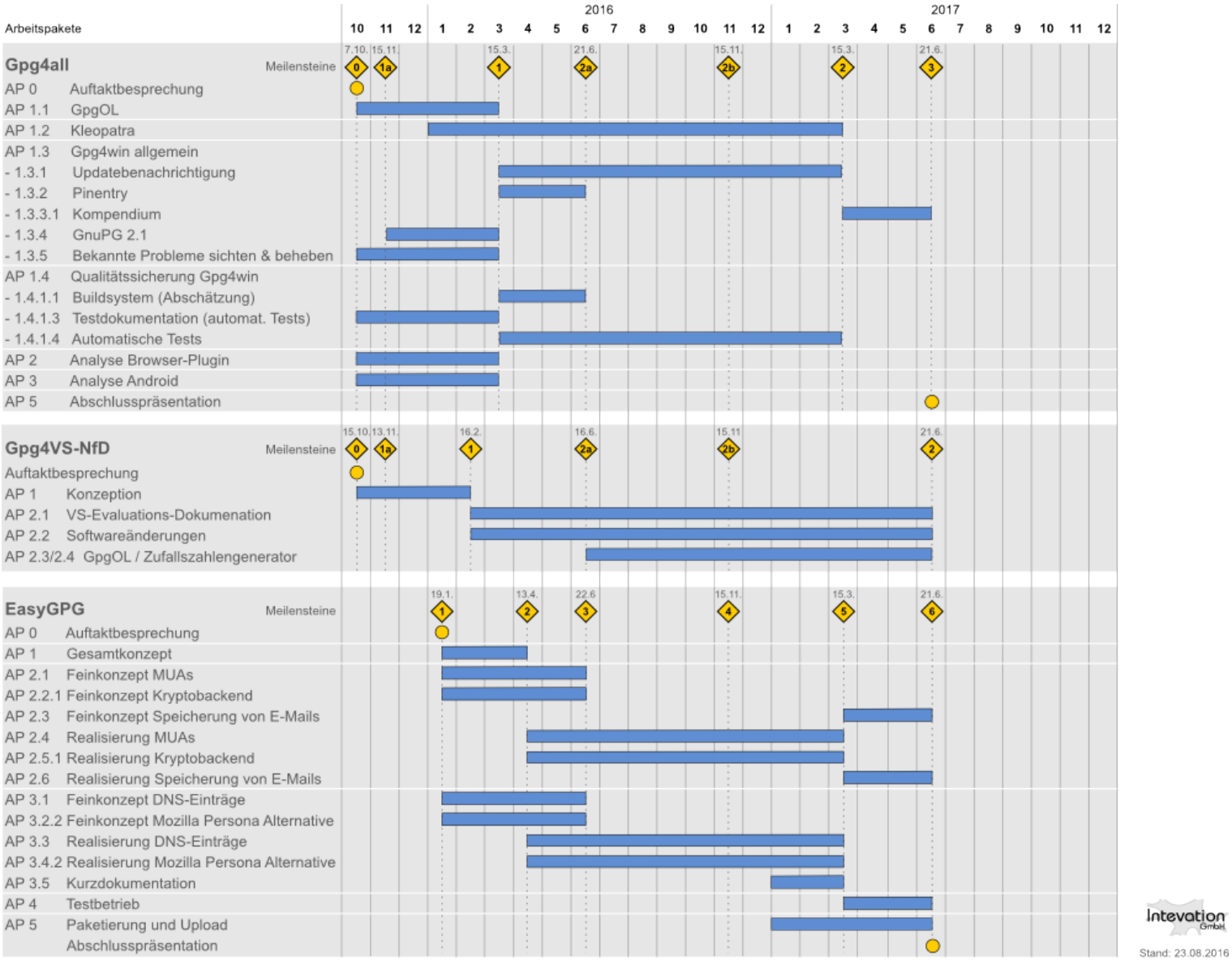
wiki.gnupg.org/BSIGuidelines

BSI TR-0202-1

- Algorithms (incl. ECC Brainpool !)
- Random Generator
- […]


Dateien signieren/verschlüsseln — Kleopatra
Für wen möchten Sie verschlüsseln?
Suchen ...
Alle Zertifikate
Name
E-Mail
Gültigkeit
Erstellt
Läuft ab
Typ
Schlüssel-Kennung
Test UserC testuserc@example.com ★ VS-konform 29.10.2010 OpenPGP 0E51F6D3
Test UserB testuserb@example.com Nicht beglaubigt 28.10.2010 OpenPGP 19D49845
Test UserA testusera@example.com Beglaubigt 28.10.2010 OpenPGP 6CFBC912
Test Selbst selbst@example.com ★ VS-konform 04.04.2016 OpenPGP EEC99E79
Hinzufügen
Entfernen
Name
E-Mail
Gültigkeit
Erstellt
Läuft ab
Typ
Schlüssel-Kennung
Test UserC testuserc@example.com ★ VS-konform 29.10.2010 OpenPGP 0E51F6D3
Test Selbst selbst@example.com ★ VS-konform 04.04.2016 OpenPGP EEC99E79
VS-konforme Kommunikation möglich.
< Back
Verschlüsseln
Cancel


Dateien signieren/verschlüsseln — Kleopatra
Für wen möchten Sie verschlüsseln?
Suchen ...
Alle Zertifikate
Name
E-Mail
Gültigkeit
Erstellt
Läuft ab
Typ
Schlüssel-Kennung
Test UserC testuserc@example.com ★ VS-konform 29.10.2010 OpenPGP 0E51F6D3
Test UserB testuserb@example.com Nicht beglaubigt 28.10.2010 OpenPGP 19D49845
Test UserA testusera@example.com Beglaubigt 28.10.2010 OpenPGP 6CFBC912
Test Selbst selbst@example.com ★ VS-konform 04.04.2016 OpenPGP EEC99E79
Hinzufügen
Entfernen
Name
E-Mail
Gültigkeit
Erstellt
Läuft ab
Typ
Schlüssel-Kennung
Test UserA testusera@example.com Beglaubigt 28.10.2010 OpenPGP 6CFBC912
Test Selbst selbst@example.com ★ VS-konform 04.04.2016 OpenPGP EEC99E79
VS-konforme Kommunikation nicht möglich.
< Back
Verschlüsseln
Cancel



Intevation GmbH

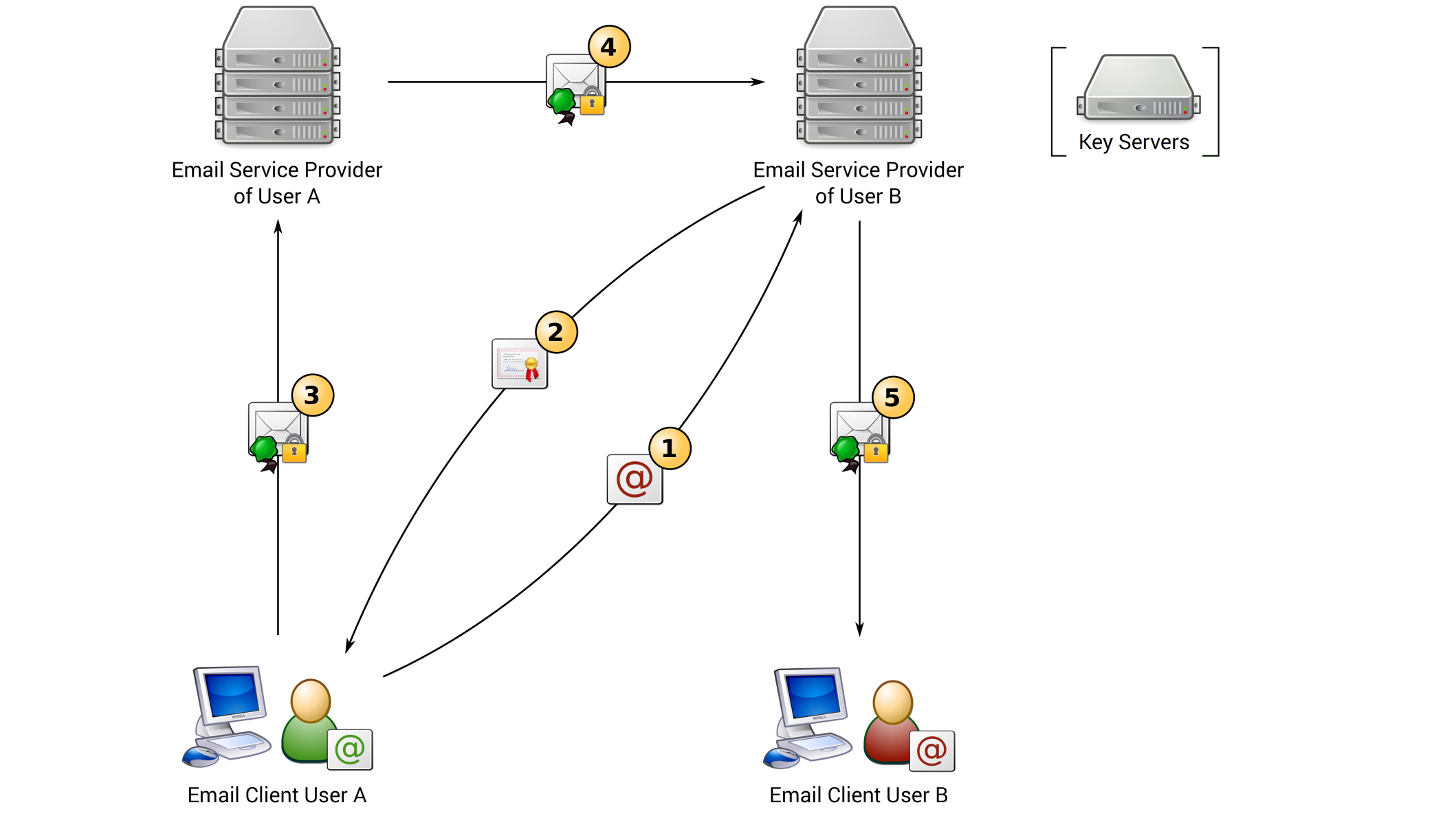
Stand: 23.08.2016

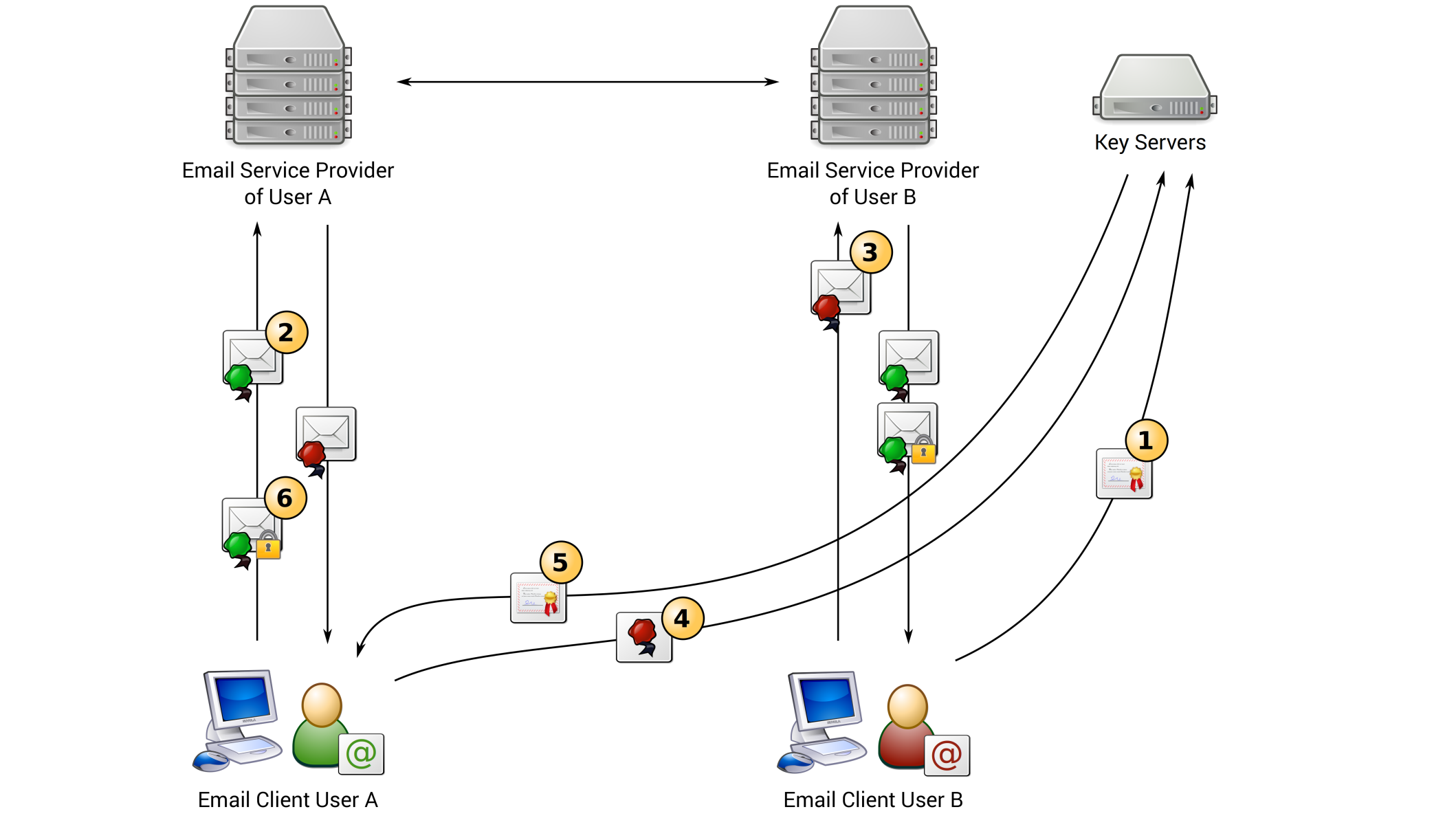
3.0

OpenPGP/MIME in Outlook (GpgOL)
ECC with GnuPG 2.2
↗UX

https://www.flickr.com/photos/funkblast/103916180 CC-BY

www.flickr.com/photos/francisco_osorio/9513730462 CC-BY


Email Service Provider
of User A
4
Email Service Provider
of User B
Key Servers
2
3
1
5
Email Client User A
Email Client User B


Email Service Provider
of User A
Email Service Provider
of User B
Key Servers
1
2
3
4
5
6
Email Client User A
Email Client User B

1. Look out for Gpg4win-Betas

2a. Convince Email providers $$

2b. Be provider. :)

3. Add it to your client

F-Droid

www.intevation.de/~bernhard