Verschlüsselte E-Mails: Wie sicher ist sicher?

- Mein Name ist **Jörg Reinhardt**
- Linux-Administrator und Support-Mitarbeiter bei der JPBerlin
- JPBerlin ist ein alteingesessener Provider mit zwei Dutzend Mitarbeitern in Berlin
- Wir machen seit über 20 Jahren Mail, gerne auch verschlüsselt
- Ich zeige Ihnen heute:
  - Warum E-Mail-Verschlüsselung selbstverständlich sein sollte
  - Mit welchen Verfahren E-Mail-Verschlüsselung umgesetzt werden kann
  - Wie einfach E-Mail-Verschlüsselung umzusetzen ist

Verschlüsselte E-Mails, wie sicher ist sicher?
[eBUSINESSLOTSE „Das Ende der E-Mail“]
Jörg Reinhardt <j.reinhardt@jpberlin.de>

JPBERLIN
POLITISCHER PROVIDER

Sichere E-Mails ab 1 € *Verschlüsselt & werbefrei*
Mailinglisten *Effektiv mailen*
Web-Hosting *Webseiten für alle*
Root-Server *Von uns umsorgt*
Die JPBerlin *Der sichere Provider*
Hilfe/FAQ *Antworten*
Blog *Aktuelles*

Die JPBerlin ist anders

- ✔ E-Mail & Web für Power-User
- ✔ Spam- und Virenschutz
- ✔ Kein Handel mit Nutzerdaten
- ✔ Konsequente Verschlüsselung
- ✔ Keine Werbebanner
- ✔ sozial & ökologisch
- ✔ persönlicher Support
- ✔ Hosting in Deutschland

Mehr über sichere E-Mails »

Mail-Postfach eröffnen

Keine Lust mehr auf große Provider mit intransparenten Interessen? Einfach mal uns ausprobieren. Mit wenigen Klicks können Sie Ihr neues Postfach in Betrieb nehmen.

Ab 1,- €/Monat. Jetzt anmelden!

JP BERLIN
POLITISCHER PROVIDER

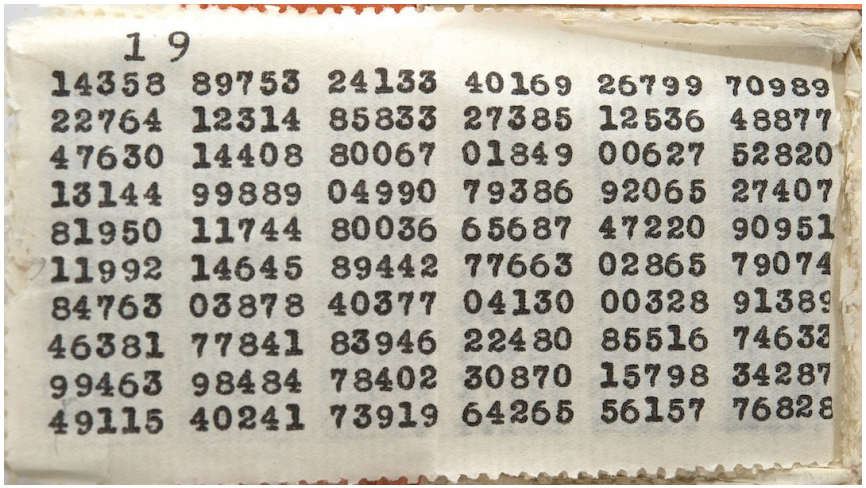
E-Mail-Verschlüsselung: Einfach und selbstverständlich

R-Znvy-Irefpuyüffryhat: Rvasnpu haq fryofgirefgäaqyvpu

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

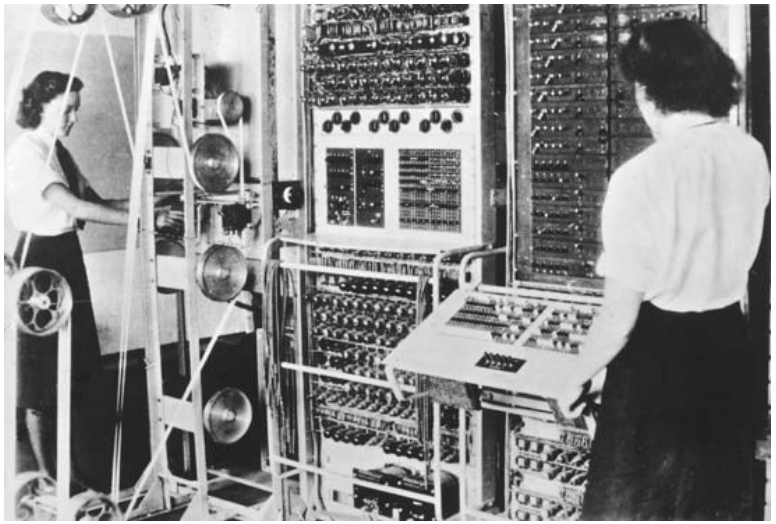
Verschlüsselung allgemein:

- Aus Klartext wird Ciphertext
- Dazu wird ein „Schlüssel“ (Passwort, Rechenverfahren) verwendet
- Nur mit Hilfe des Schlüssels kann der Ciphertext wieder in Klartext verwandelt werden



Sicherheit und Komplexität

- Wann ist eine Nachricht sicher verschlüsselt?
  - Bei ausreichender und guter Schlüssellänge
  - Bei ausreichender Komplexität des Verfahrens



SSL und TLS:
Die Transportverschlüsselung

- E-Mails, Webseiten und andere Daten werden von Rechner zu Rechner durch das Internet geleitet
- Daten werden repliziert und automatisiert mitgelesen
- SSL/TLS stellt eine Transportverschlüsselung zwischen zwei Rechnern sicher
  - Bekannt als „https“ bei Webseiten
  - Im Mail-Client als „SSL“ oder „STARTTLS“ benannt („Pop3s“, „IMAPs“)
- Zwischen zwei Übertragungen liegt die E-Mail aber unverschlüsselt auf den Servern

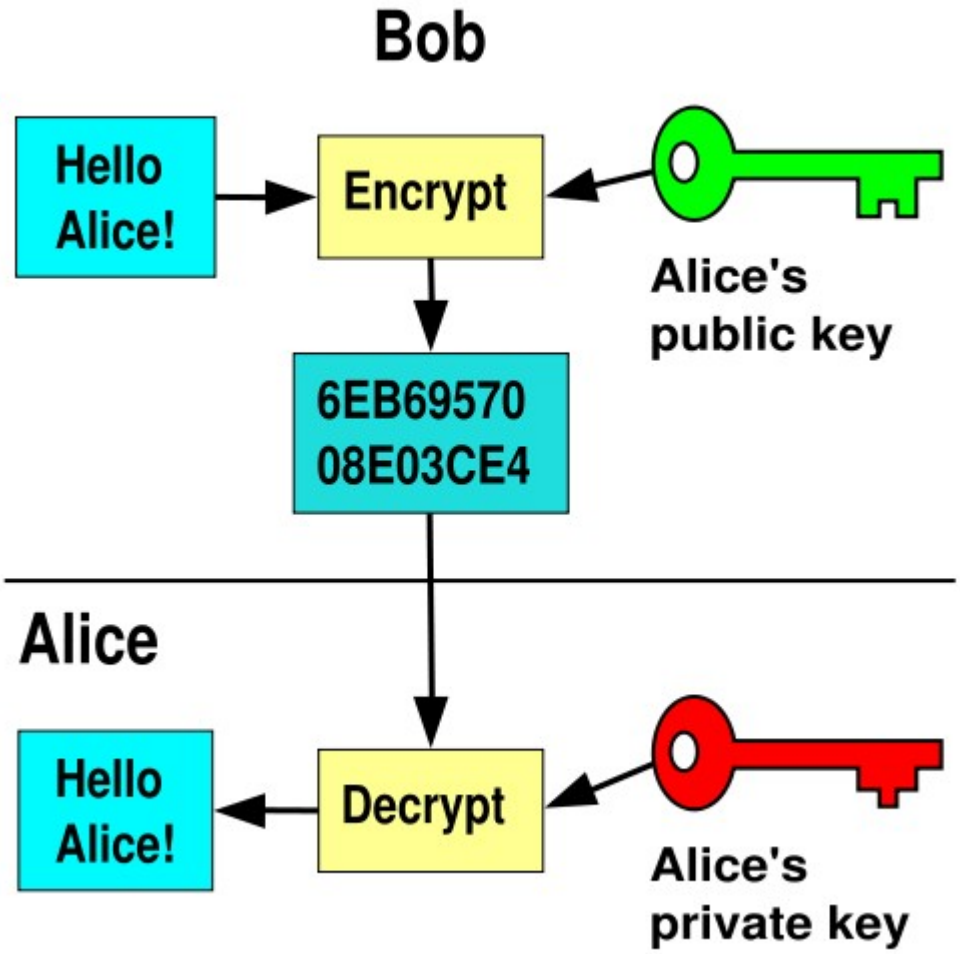
Die Transportverschlüsselung im Mail-Client

- Eine E-Mail-Übertragung erfolgt in mehreren Einzelschritten
  - Vom Mailprogramm zum Provider des Versenders
  - Vom Provider des Versenders zum Provider des Empfängers
  - Vom Provider des Empfängers zum Mailprogramm
- SSL/TLS-Verschlüsselung zwischen Ihrem Mailprogramm und dem Mailserver des Providers können Sie leicht aktivieren.
- Ob Provider untereinander verschlüsseln können Sie nicht beeinflussen

Symmetrische und asymmetrische Verschlüsselung

- Symmetrische Verschlüsselung
  - Die Schlüssel müssen vor der Kommunikation ausgetauscht werden
  - Beim Austausch kann der Schlüssel kopiert werden und in die falschen Hände geraten
- Asymmetrische Verschlüsselung
  - Eine Nachricht die mit einem Public Key verschlüsselt wurde, kann nur mit dem dazugehörigen Private Key entschlüsselt werden
  - Nur der Public Key muss ausgetauscht werden
  - Fällt der Public Key in falsche Hände, bleibt die Nachricht trotzdem sicher

public/private key pair



So läuft die Verschlüsselung in Ihrem Mailprogramm

- Installieren Sie ein PGP-Plugin (Bspw. Enigmail)
- Erzeugen Sie ein Schlüsselpaar
- Ihr öffentlicher Schlüssel kann, darf und soll überall bekannt sein
  - Veröffentlichen Sie Ihren Schlüssel auf den Keyservern
- Wer Ihnen schreiben möchte, verwendet Ihren Public Key
  - Wenn Sie schreiben möchten, verwenden Sie den Public Key des Empfängers. Sie finden Ihn auf den Keyservern
  - Ein gutes Mailprogram macht das unbemerkt im Hintergrund
- Das wirft zwei Fragen auf:
  - Wie werden die Public Keys verteilt? (Keyserver)
  - Wie kann ich sicher sein, das ein Public Key wirklich der Person gehört, der ich schreiben will?

Keyserver

- Für die Verteilung der Public Keys existiert ein Netz von Keyservern
- Sie müssen Ihren Key nur auf einen Keyserver hochladen
  - Die Keyserver tauschen die veröffentlichten Keys untereinander aus
  - Es ist egal auf welchem Keyserver Sie einen Public Key suchen. Jeder Public Key sollte auf allen Keyservern zu finden sein.
- Ein Key gehört immer zu einer E-Mail-Adresse
- Sie suchen auf den Keyservern nach der Adresse des Empfängers

Zertifikate und Signaturen

- Asymmetrische Schlüssel können nicht nur verschlüsseln. Sie können auch signieren („unterschreiben“).
  - Die **Orginalität** und **Unversehrtheit** einer Nachricht kann eindeutig sichergestellt werden
  - Die **Herkunft** kann eindeutig sicher gestellt werden
- Diese Eigenschaften helfen einen privaten Schlüssel zu verifizieren
  - Ein Schlüssel kann von einer dritten Person signiert sein, der ich bereits vertraue
  - Die vertrauenswürdige Person zertifiziert damit die Echtheit des Schlüssels
  - Dazu muss ich vorher den Public Key der vertrauenswürdigen Person besitzen und sicher sein, dass dieser echt ist
  - Es bildet sich eine Vertrauensnetzwerk („web of trust“)

Eine PGP-Signatur unter einer E-Mail

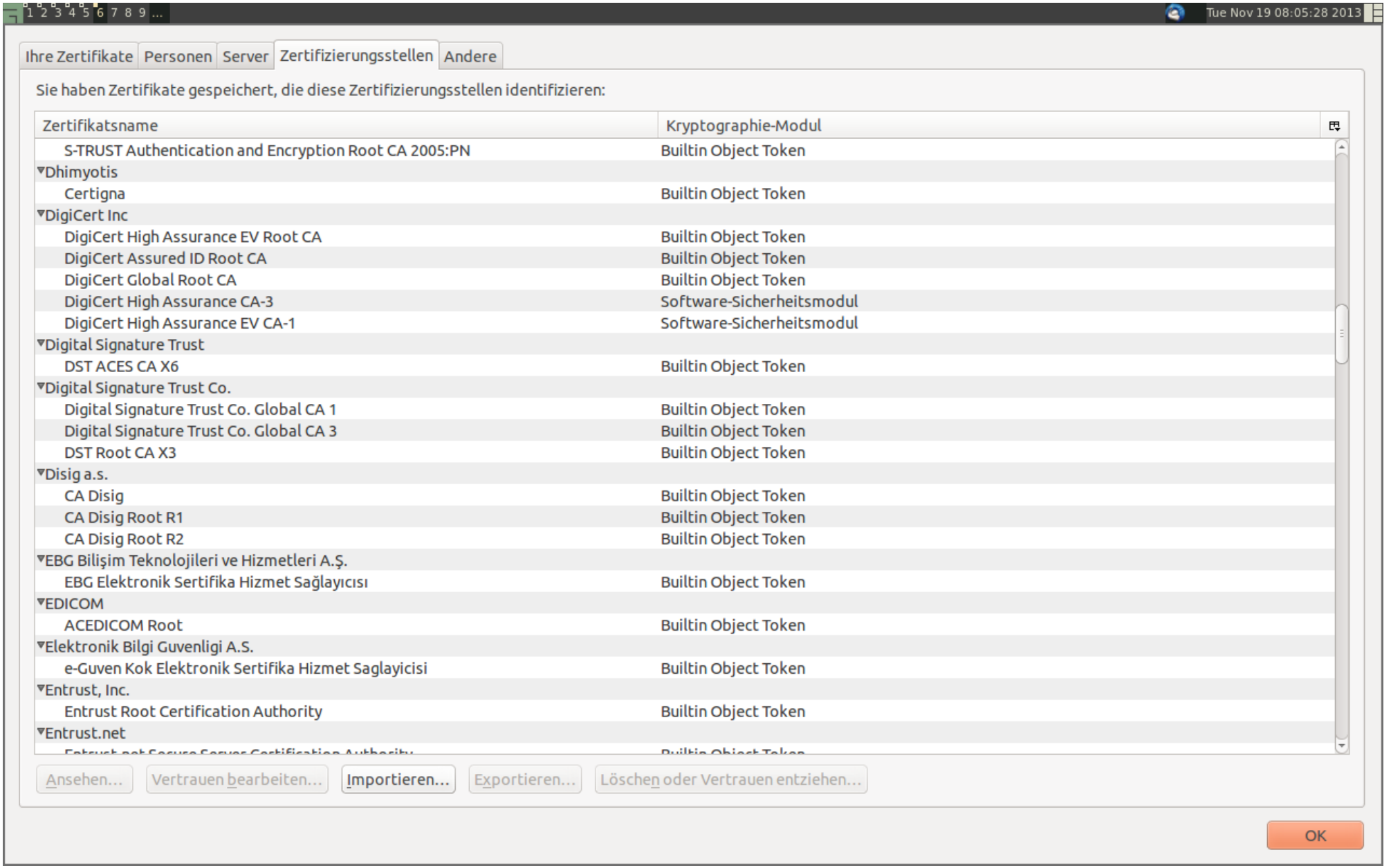
```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.12 (GNU/Linux)
Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/

iQIcBAEBAgAGBQJSi0KzAAoJEPQQeQp7JEgDgn8P/0VnfgimCMKP3sr8UJ+o6ZC5
9LeUNRLP6c/Bd5KdwSHhfef/SLeYVuLVtH84szGvMqcSnU7LuKKcX+ftlLU5W2R6
/fasNO6KrYvotqz1GaTYN3PVZyXZIrFnMEN8QgZL7zGl+IzbqBlVbLVPUzLf+Scf
wEuQKQMUmqFRANz7x17SFrgE9Ou2LhtyWgvxJG+L5TQZ1YVpen27bgDK8OMgn2Kp
eSV6lsObn3L5+IGSrlKqnEG/RJdMw3EKEc9loJekCwMPo0WP52Zo+B9ZJo5gU5Q2
uACXcAAmHBq1ZRqLSX2iyz89kZperB0XuHR0JTNztQfx4JeIqjxUOSeGk+m5jPur
106M/WCUmrdO8ISHojB+Oi0Q1SnBHofxSIQ/M8hTgk87gXQSq+KolqWoDNtGy3oN
lYuIJ07p9tm4rtxgy9VPTq9v/OB8hnCwc3QpqVJr3P4FvRhHyl4Zl4nTzurgi6RV
fwARhN3UJzBbGdl2p+gq3uI2FyNP8N2XIGIv99ENCX8czbWnqe03oNfrUuIHnIKB
mXskhH2PW5A4Phr/c3p6wG1sbLm+JrpvtR9UBTccwDVnTOqoTECAGn5i/sp7yfS+
+fQa+70X0ZbTnq5OveygMMxKZykp76ATyq3oYCyHAGFOwEBgWrQ7jrwVDXG61FkR
2k7SKdP4TVowO9FUW2cx
=3yQH
-----END PGP SIGNATURE-----

--v7O9LJBWdeJKW6l63EDf4kaWUrTqu0B7l--
```

Vertrauen

- GPG/PGP
  - Benutzerschlüssel werden mit Benutzerschlüsseln signiert
  - Verantwortung liegt bei den Benutzern
  - Ich kann wählen, wem ich trauen möchte
  - Je größer das Netz wird, desto schwieriger wird es, einen Schlüssel zu fälschen
  - Unabhängig von Dritten
  - Kostenlos
- S/MIME
  - Schlüssel werden von Zertifizierungsstellen (CAs) signiert
  - Verantwortung liegt bei den Zertifizierungsstellen
  - Keine Wahl, wem ich trauen möchte, die Liste der Zertifizierungsstellen ist vorinstalliert
  - Wird eine CA kompromittiert, sind alle Schlüssel unsicher
  - Abhängigkeit von der CA
  - Kostspielig

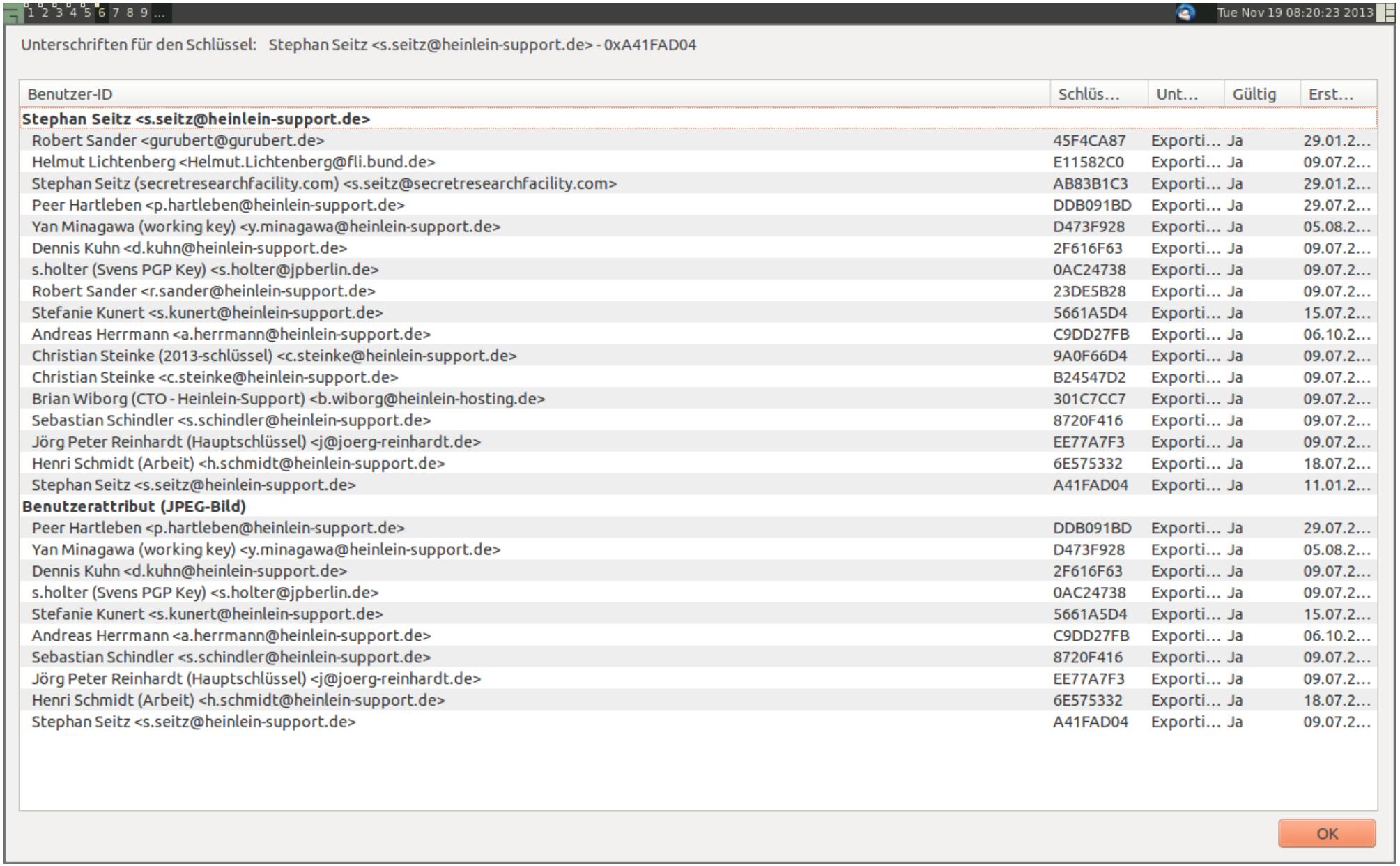
JP BERLIN
POLITISCHER PROVIDER

Verschlüsselte E-Mails, wie sicher ist sicher?
[eBUSINESSLOTSE „Das Ende der E-Mail“]
Jörg Reinhardt <j.reinhardt@jpberlin.de>



JP BERLIN
POLITISCHER PROVIDER

Verschlüsselte E-Mails, wie sicher ist sicher?
[eBUSINESSLOTSE „Das Ende der E-Mail“]
Jörg Reinhardt <j.reinhardt@jpberlin.de>

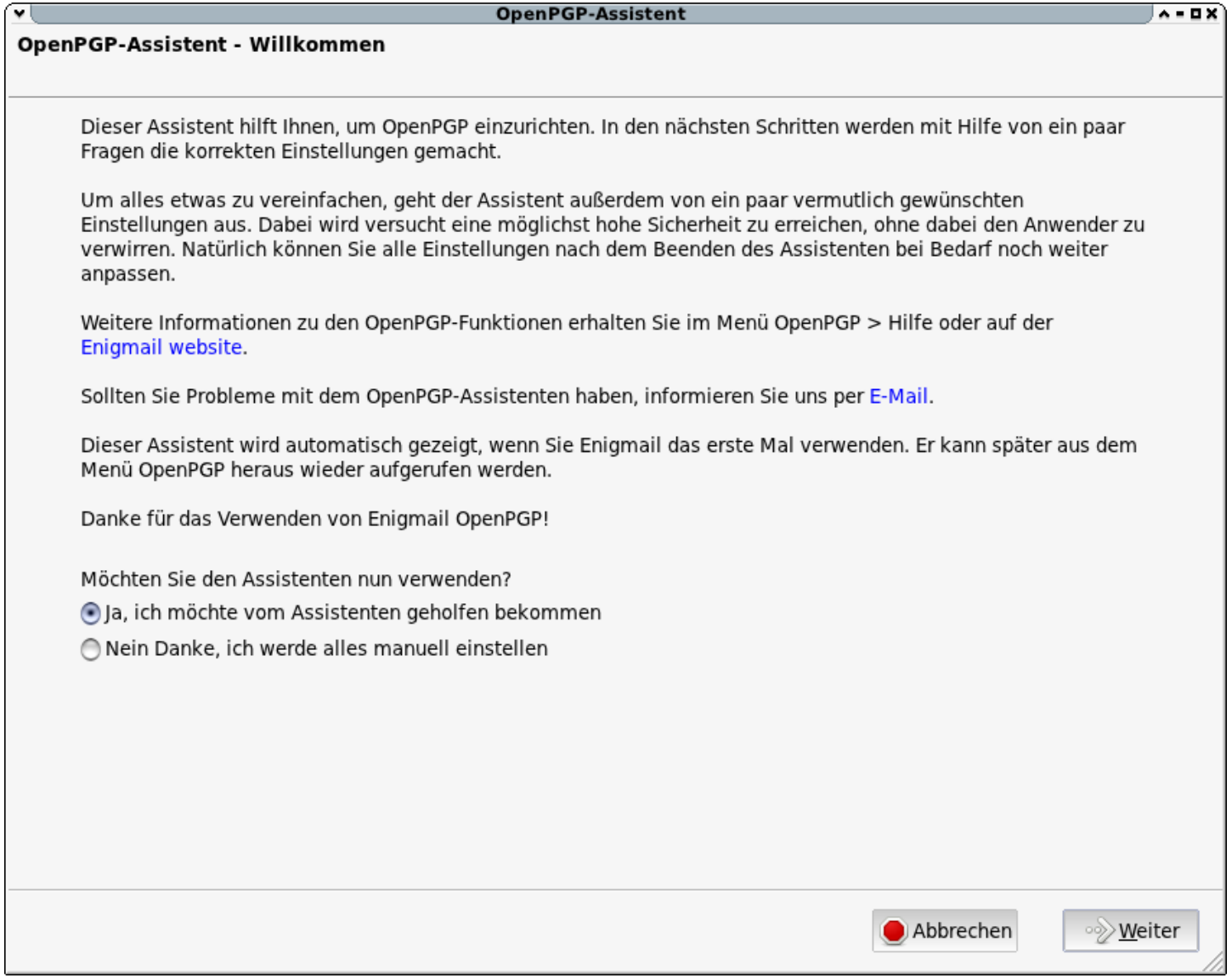


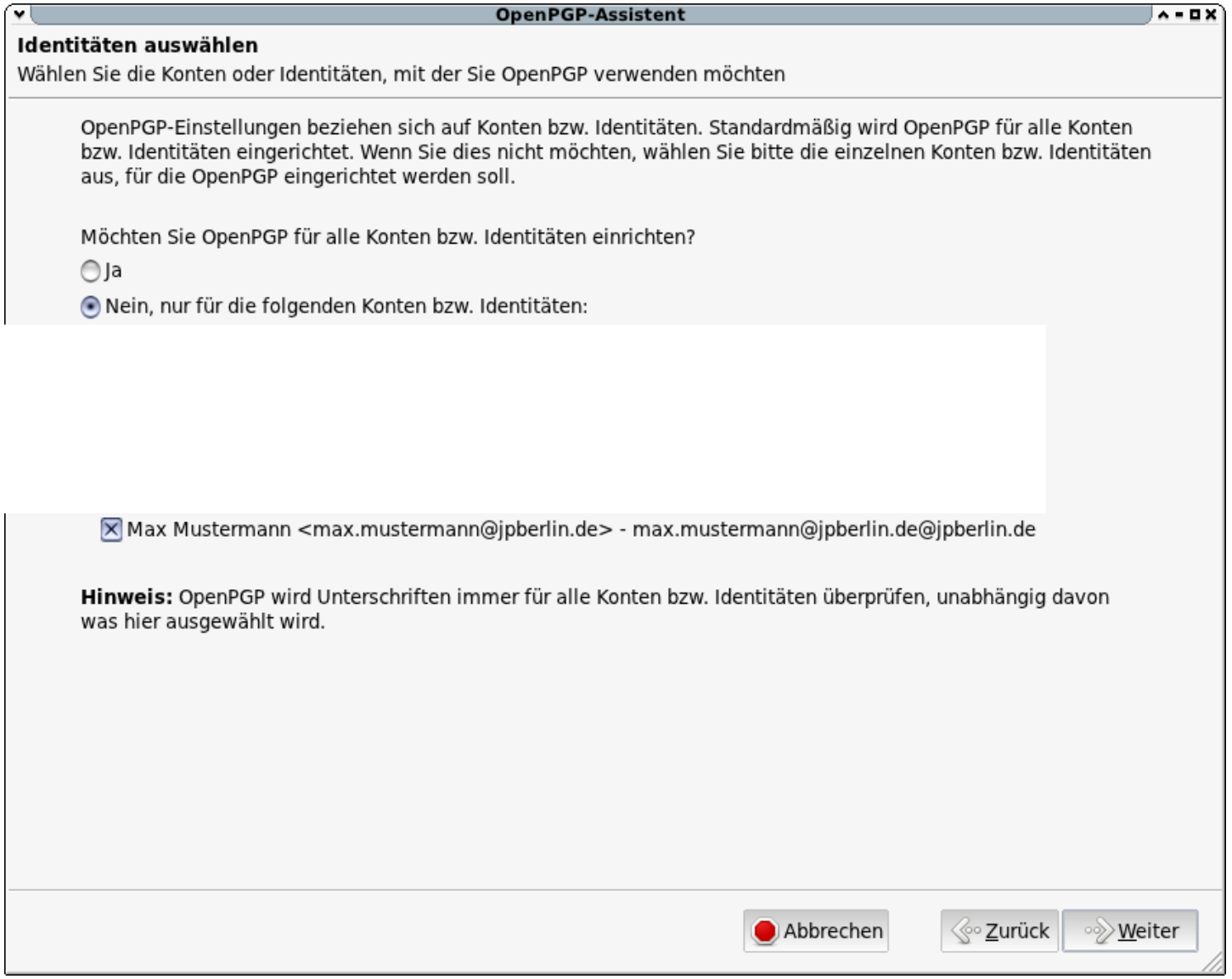
Offene vs. „geschützte" Verfahren

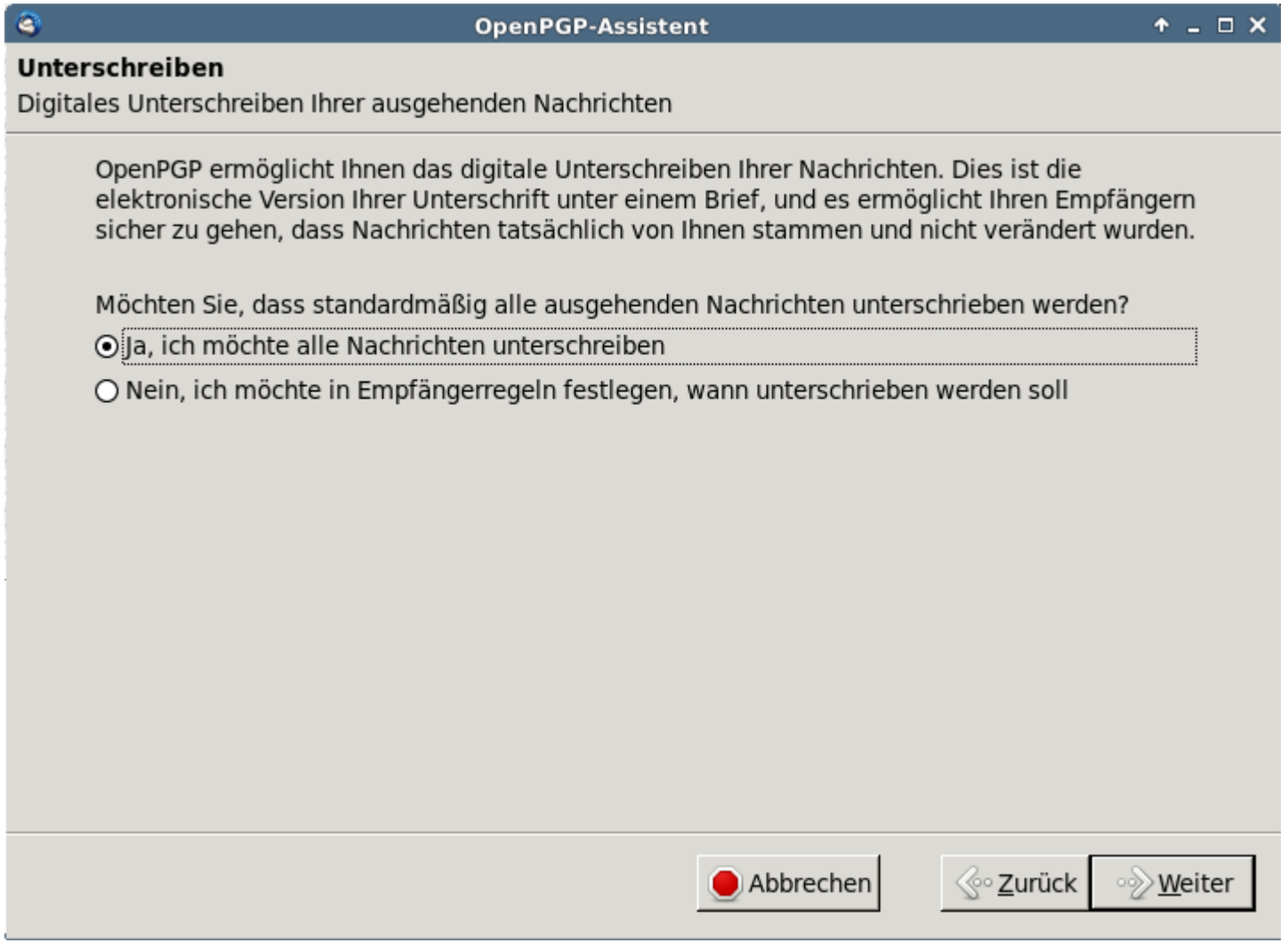
- Verschlüsselungsverfahren müssen öffentlich sein!
  - Nur ein öffentliches Verfahren kann unabhängig getestet und geprüft werden
  - Wenn die vermeintliche Sicherheit auf einem Geheimnis beruht, kann es auch einen geheimen Weg geben, diese zu umgehen
  - Nur Verfahren, die sicher bleiben, obwohl ihre Funktionsweise bekannt ist, sind wirklich sicher
    - Jeder kann in Erfahrung bringen, wie Sicherheitsschlösser funktionieren
    - Deswegen bleibt es trotzdem schwierig, Sicherheitsschlösser zu öffnen
  - Verschlüsselungsverfahren sollten nicht patentiert sein und niemandem „gehören“
    - Was machen Sie mit den verschlüsselten Daten, wenn der Hersteller Ihrer Sicherheitssoftware Konkurs anmeldet?

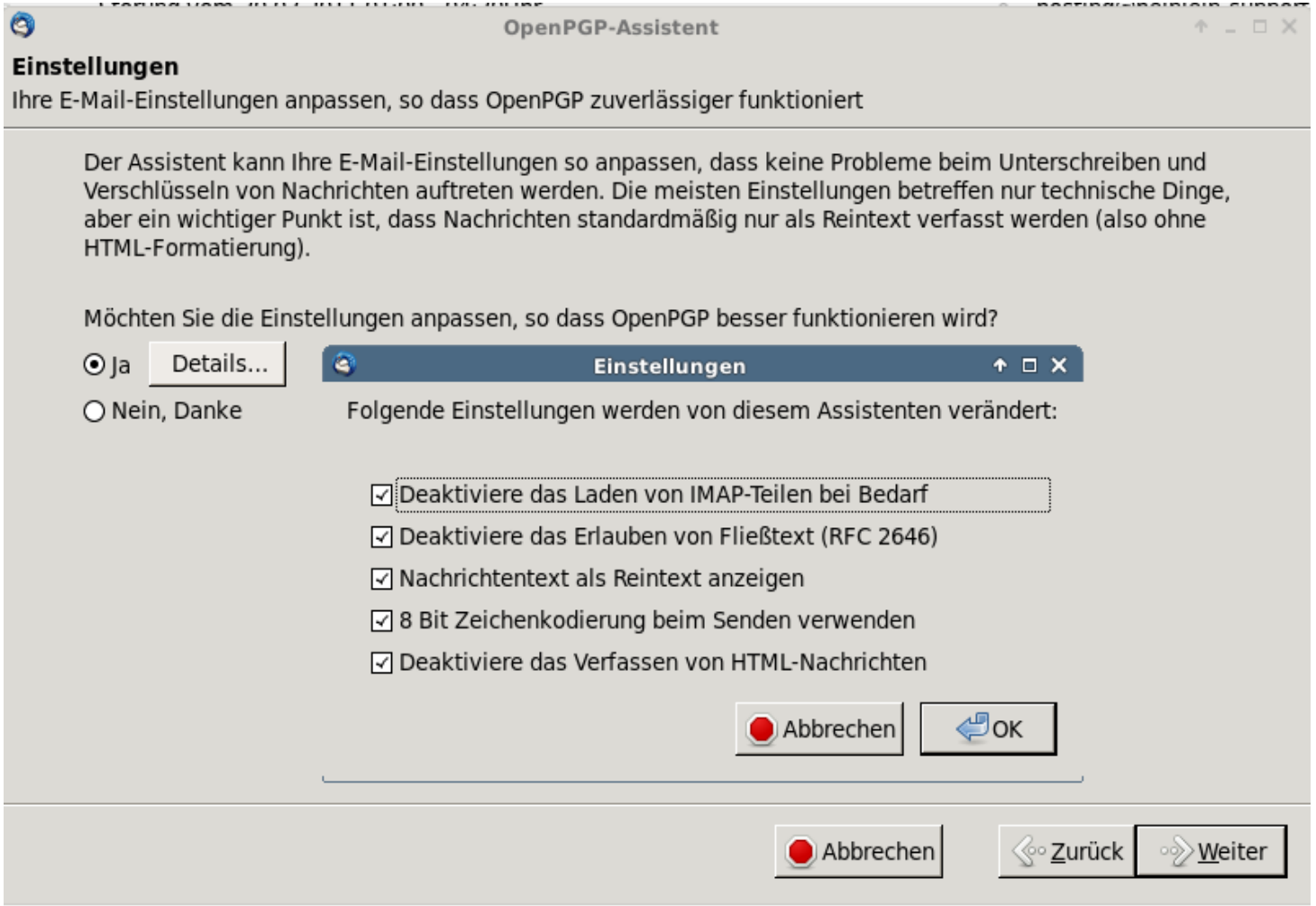
Verschlüsselte E-Mails, wie sicher ist sicher?
[eBUSINESSLOTSE „Das Ende der E-Mail“]
Jörg Reinhardt <j.reinhardt@jpberlin.de>

Die Einrichtung von PGP/GPG im Schnelldurchlauf

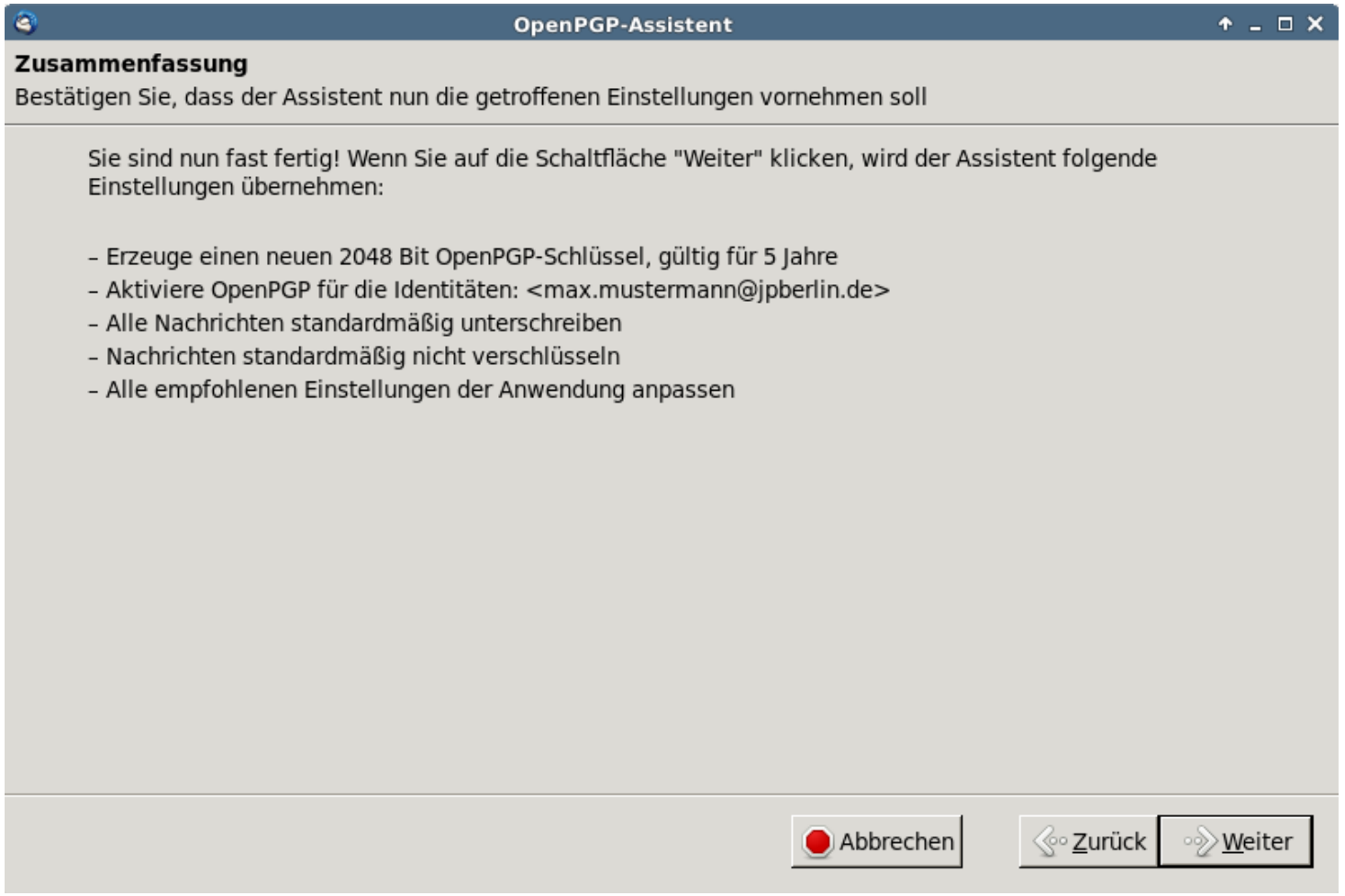

OpenPGP-Assistent
OpenPGP-Assistent - Willkommen
Dieser Assistent hilft Ihnen, um OpenPGP einzurichten. In den nächsten Schritten werden mit Hilfe von ein paar Fragen die korrekten Einstellungen gemacht.
Um alles etwas zu vereinfachen, geht der Assistent außerdem von ein paar vermutlich gewünschten Einstellungen aus. Dabei wird versucht eine möglichst hohe Sicherheit zu erreichen, ohne dabei den Anwender zu verwirren. Natürlich können Sie alle Einstellungen nach dem Beenden des Assistenten bei Bedarf noch weiter anpassen.
Weitere Informationen zu den OpenPGP-Funktionen erhalten Sie im Menü OpenPGP > Hilfe oder auf der Enigmail website.
Sollten Sie Probleme mit dem OpenPGP-Assistenten haben, informieren Sie uns per E-Mail.
Dieser Assistent wird automatisch gezeigt, wenn Sie Enigmail das erste Mal verwenden. Er kann später aus dem Menü OpenPGP heraus wieder aufgerufen werden.
Danke für das Verwenden von Enigmail OpenPGP!
Möchten Sie den Assistenten nun verwenden?
Ja, ich möchte vom Assistenten geholfen bekommen
Nein Danke, ich werde alles manuell einstellen
Abbrechen
Weiter

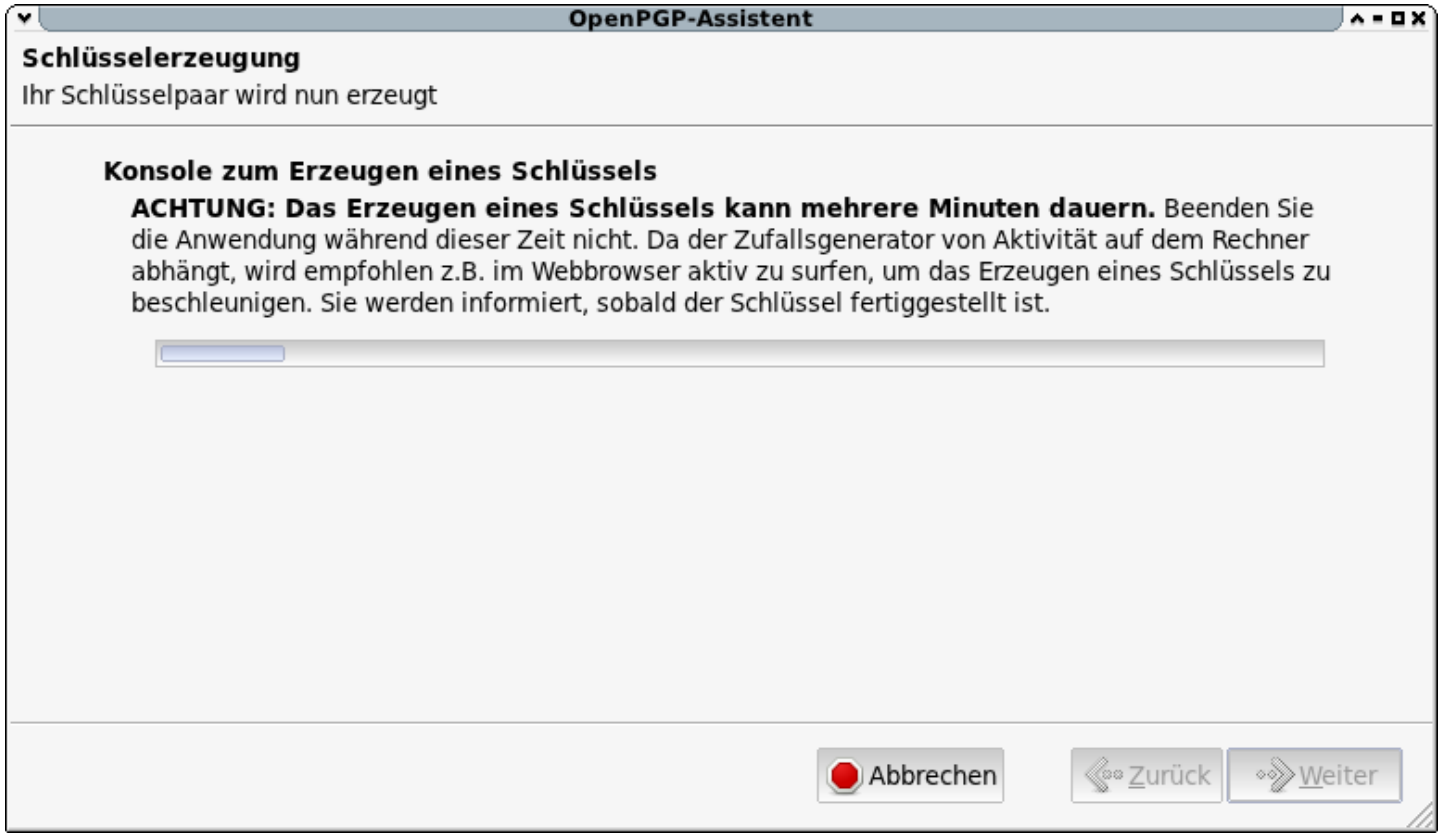

OpenPGP-Assistent
Identitäten auswählen
Wählen Sie die Konten oder Identitäten, mit der Sie OpenPGP verwenden möchten
OpenPGP-Einstellungen beziehen sich auf Konten bzw. Identitäten. Standardmäßig wird OpenPGP für alle Konten bzw. Identitäten eingerichtet. Wenn Sie dies nicht möchten, wählen Sie bitte die einzelnen Konten bzw. Identitäten aus, für die OpenPGP eingerichtet werden soll.
Möchten Sie OpenPGP für alle Konten bzw. Identitäten einrichten?
Ja
Nein, nur für die folgenden Konten bzw. Identitäten:
Max Mustermann <max.mustermann@jpberlin.de> - max.mustermann@jpberlin.de@jpberlin.de
Hinweis: OpenPGP wird Unterschriften immer für alle Konten bzw. Identitäten überprüfen, unabhängig davon was hier ausgewählt wird.
Abbrechen
Zurück
Weiter


OpenPGP-Assistent
Unterschreiben
Digitales Unterschreiben Ihrer ausgehenden Nachrichten
OpenPGP ermöglicht Ihnen das digitale Unterschreiben Ihrer Nachrichten. Dies ist die elektronische Version Ihrer Unterschrift unter einem Brief, und es ermöglicht Ihren Empfängern sicher zu gehen, dass Nachrichten tatsächlich von Ihnen stammen und nicht verändert wurden.
Möchten Sie, dass standardmäßig alle ausgehenden Nachrichten unterschrieben werden?
Ja, ich möchte alle Nachrichten unterschreiben
Nein, ich möchte in Empfängerregeln festlegen, wann unterschrieben werden soll
Abbrechen
Zurück
Weiter

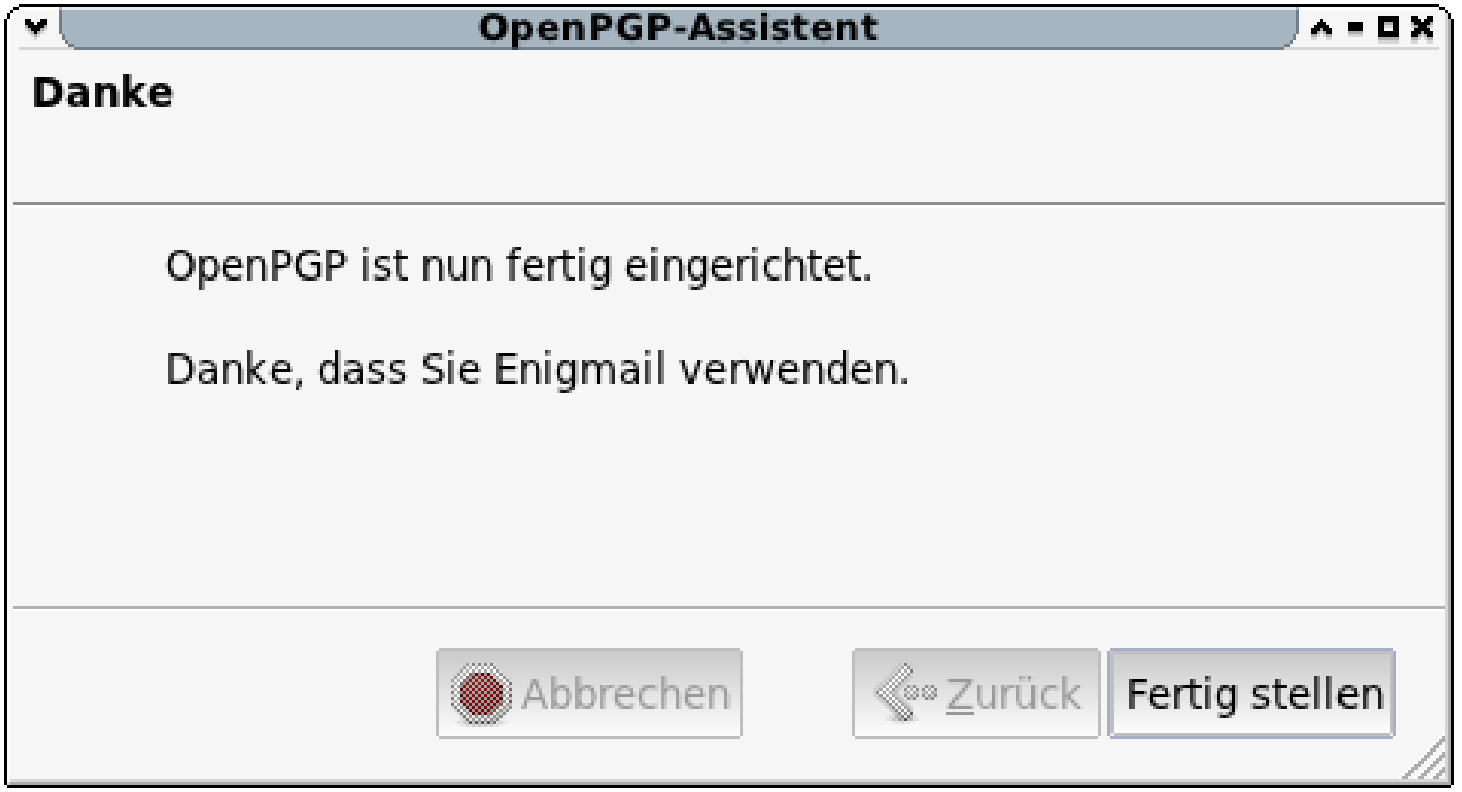

OpenPGP-Assistent
Einstellungen
Ihre E-Mail-Einstellungen anpassen, so dass OpenPGP zuverlässiger funktioniert
Der Assistent kann Ihre E-Mail-Einstellungen so anpassen, dass keine Probleme beim Unterschreiben und Verschlüsseln von Nachrichten auftreten werden. Die meisten Einstellungen betreffen nur technische Dinge, aber ein wichtiger Punkt ist, dass Nachrichten standardmäßig nur als Reintext verfasst werden (also ohne HTML-Formatierung).
Möchten Sie die Einstellungen anpassen, so dass OpenPGP besser funktionieren wird?
Ja
Details...
Nein, Danke
Einstellungen
Folgende Einstellungen werden von diesem Assistenten verändert:
Deaktiviere das Laden von IMAP-Teilen bei Bedarf
Deaktiviere das Erlauben von Fließtext (RFC 2646)
Nachrichtentext als Reintext anzeigen
8 Bit Zeichenkodierung beim Senden verwenden
Deaktiviere das Verfassen von HTML-Nachrichten
Abbrechen
OK
Abbrechen
Zurück
Weiter

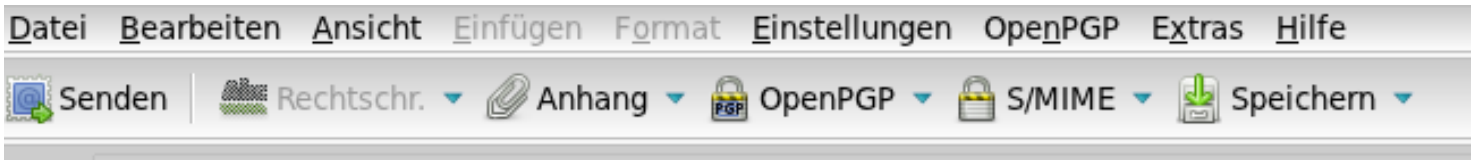

OpenPGP-Assistent
OpenPGP-Schlüssel erzeugen
Erzeugen eines Schlüssels zum Unterschreiben und Verschlüsseln
Sie benötigen ein "Schlüsselpaar", um Nachrichten unterschreiben und verschlüsseln zu können. Ein Schlüsselpaar besteht aus einem öffentlichen Schlüssel und einem privaten Schlüssel.
Ihren öffentlichen Schlüssel (das Vorhängeschloss) müssen Sie allen Personen geben, die Ihre Unterschrift überprüfen und Nachrichten verschlüsselt an Sie senden können sollen. Im Gegensatz dazu müssen Sie Ihren privaten Schlüssel geheim halten! Sie dürfen diesen NICHT weitergeben oder ungeschützt lassen. Mit Hilfe Ihres privaten Schlüssels kann man alle Nachrichten lesen, die verschlüsselt an Sie gesendet wurden. Außerdem kann man damit in Ihrem Namen unterschreiben! Der private Schlüssel wird deshalb von einer Passphrase geschützt.
Benutzer-ID:
Max Mustermann <max.mustermann@jpberlin.de> - max.mustermann@jpberlin.de@jpberlin.de
Passphrase
Bitte bestätigen Sie Ihre Passphrase durch erneutes Eingeben
Abbrechen
Zurück
Weiter

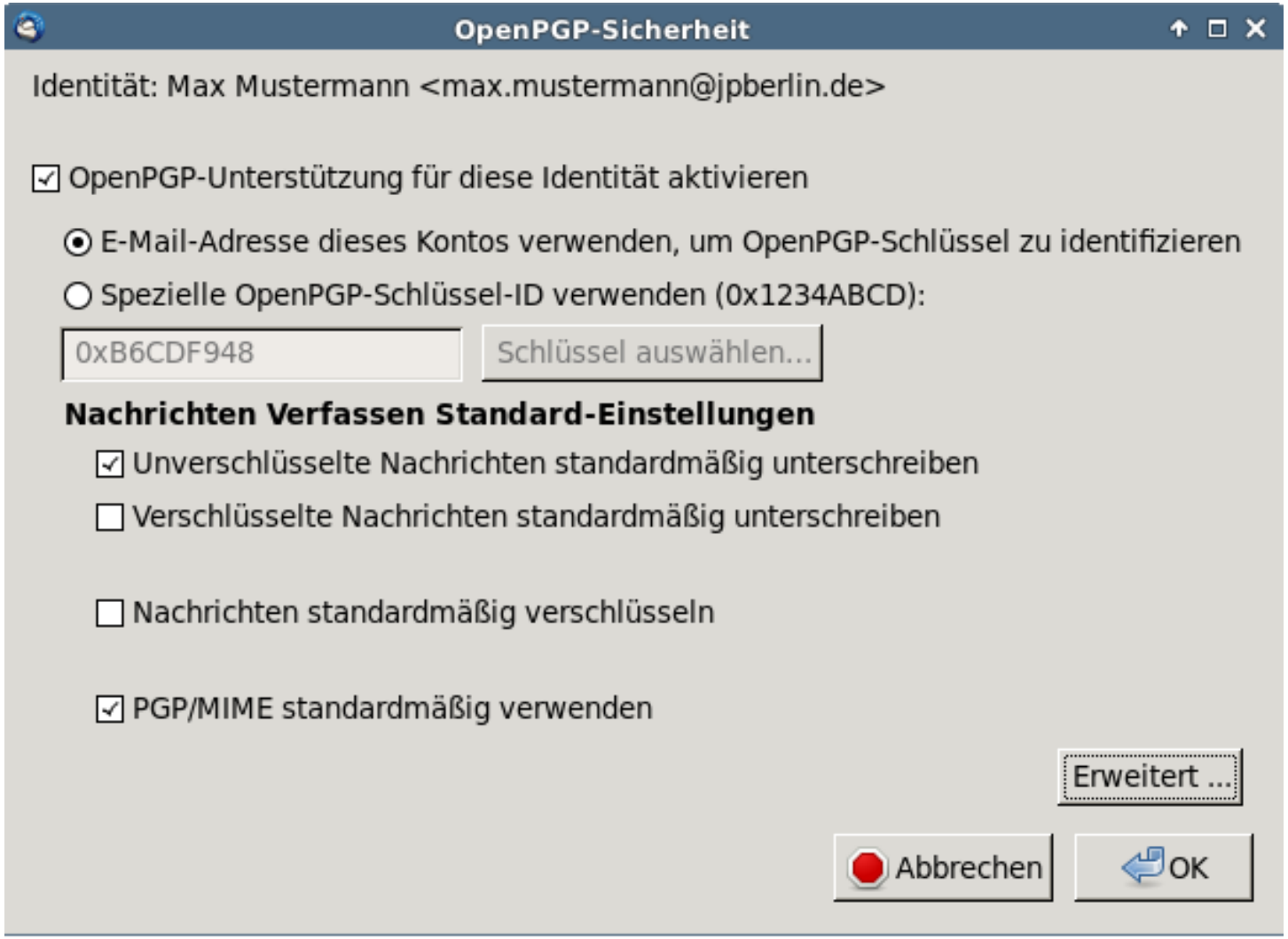

OpenPGP-Assistent
Zusammenfassung
Bestätigen Sie, dass der Assistent nun die getroffenen Einstellungen vornehmen soll
Sie sind nun fast fertig! Wenn Sie auf die Schaltfläche "Weiter" klicken, wird der Assistent folgende Einstellungen übernehmen:
– Erzeuge einen neuen 2048 Bit OpenPGP-Schlüssel, gültig für 5 Jahre
– Aktiviere OpenPGP für die Identitäten: <max.mustermann@jpberlin.de>
– Alle Nachrichten standardmäßig unterschreiben
– Nachrichten standardmäßig nicht verschlüsseln
– Alle empfohlenen Einstellungen der Anwendung anpassen
Abbrechen
Zurück
Weiter

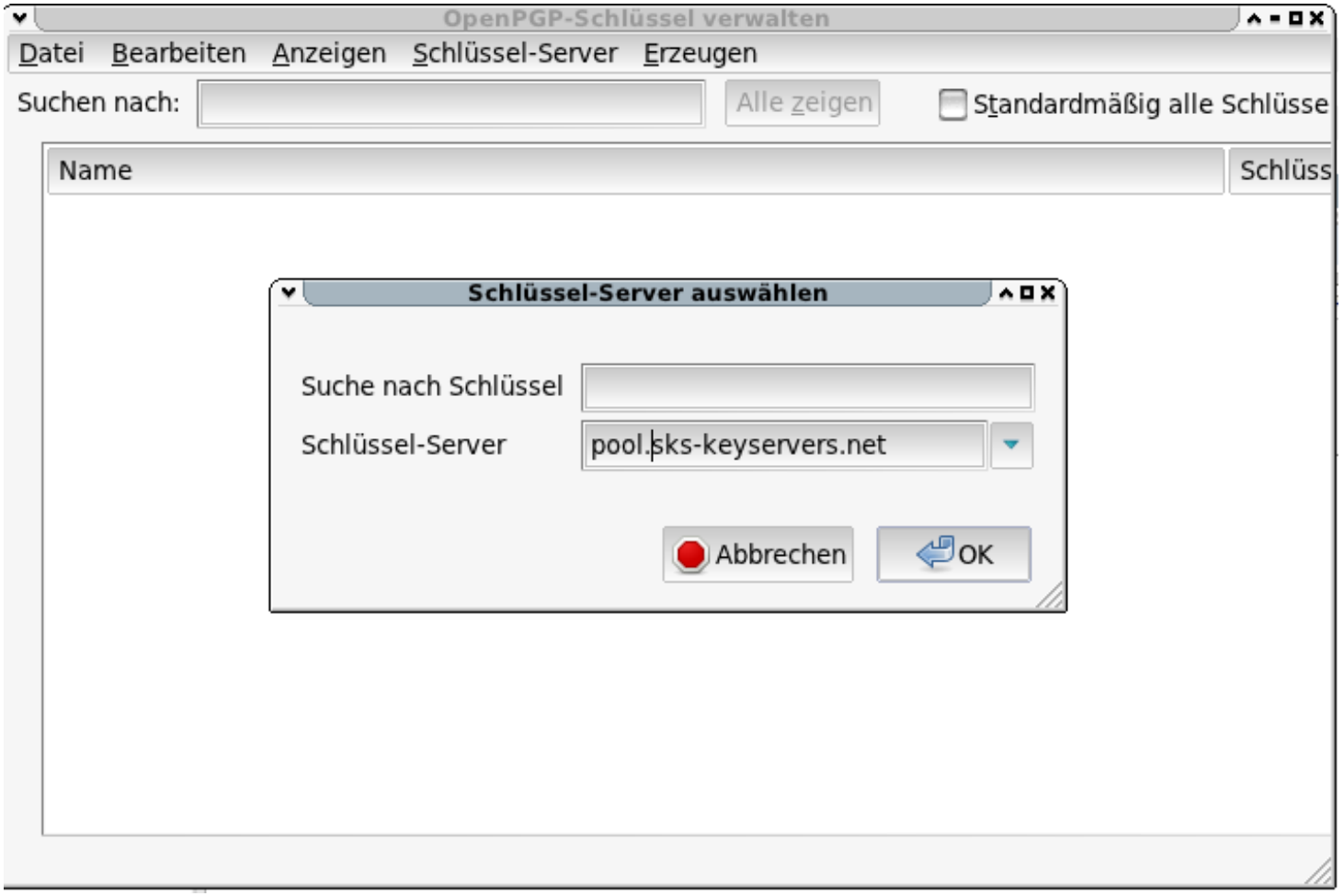

OpenPGP-Assistent
Schlüsselerzeugung
Ihr Schlüsselpaar wird nun erzeugt
Konsole zum Erzeugen eines Schlüssels
ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern. Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.
Abbrechen
Zurück
Weiter

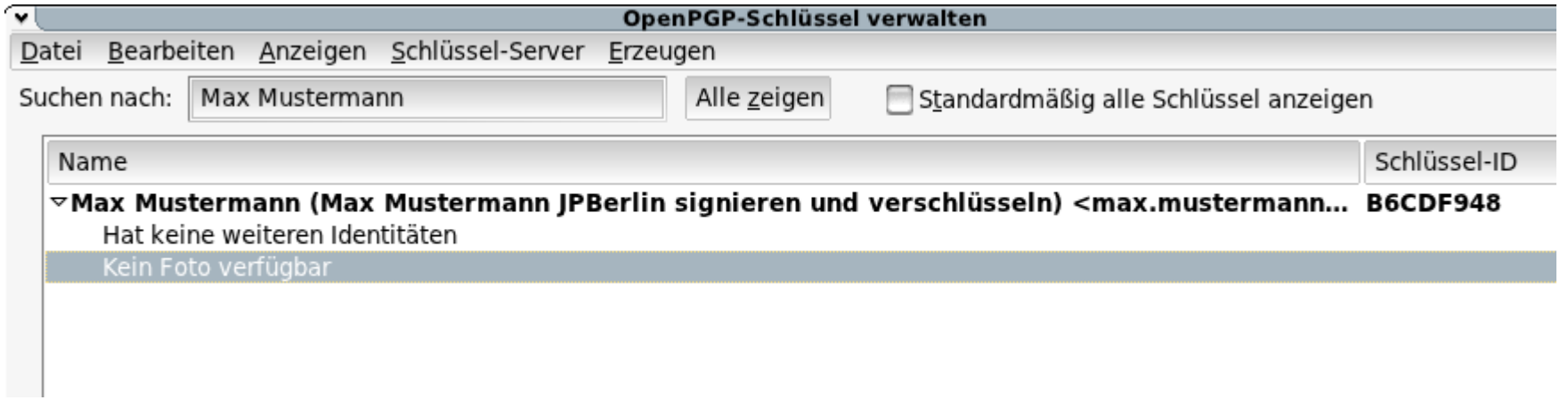

OpenPGP-Assistent
Schlüsselerzeugung
Ihr Schlüsselpaar wird nun erzeugt
Konsole zum Erzeugen eines Schlüssels
ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern. Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.
OpenPGP-Bestätigung
Erzeugen des Schlüssels abgeschlossen. Benutzer-ID <max.mustermann@jpberlin.de> wird zum Unterschreiben verwendet.
Es wird dringend empfohlen, dass Sie nun ein Widerrufszertifikat für Ihren Schlüssel erzeugen. Dieses Zertifikat benötigen Sie, um Ihren Schlüssel bei Bedarf für ungültig zu erklären (z.B. wenn der Schlüssel missbraucht, verloren oder gestohlen wird).
Möchten Sie nun das zugehörige Widerrufszertifikat erzeugen?
Überspringen
Zertifikat erzeugen
Abbrechen
Zurück
Weiter

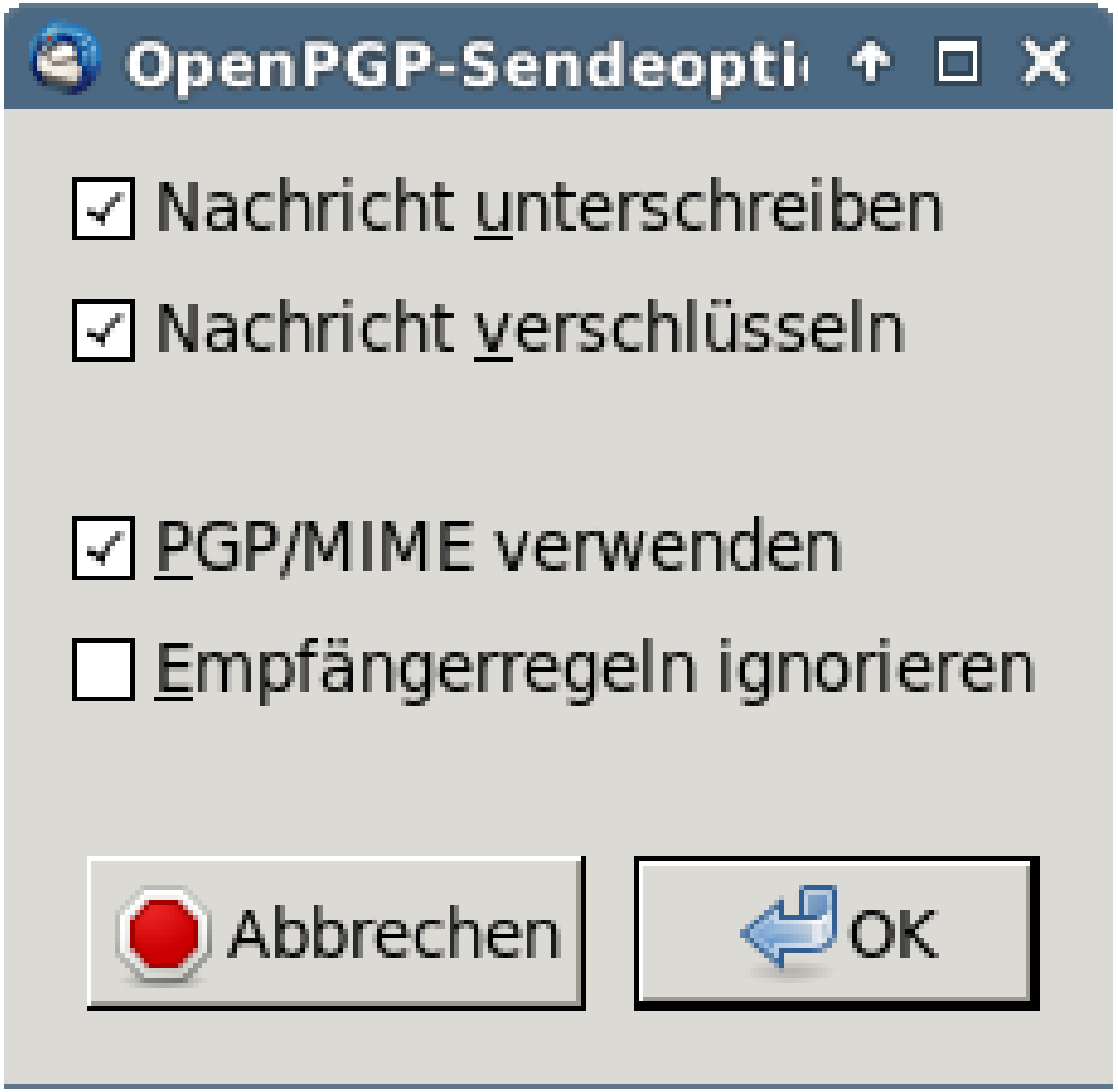

OpenPGP-Assistent
Danke
OpenPGP ist nun fertig eingerichtet.
Danke, dass Sie Enigmail verwenden.
Abbrechen
Zurück
Fertig stellen

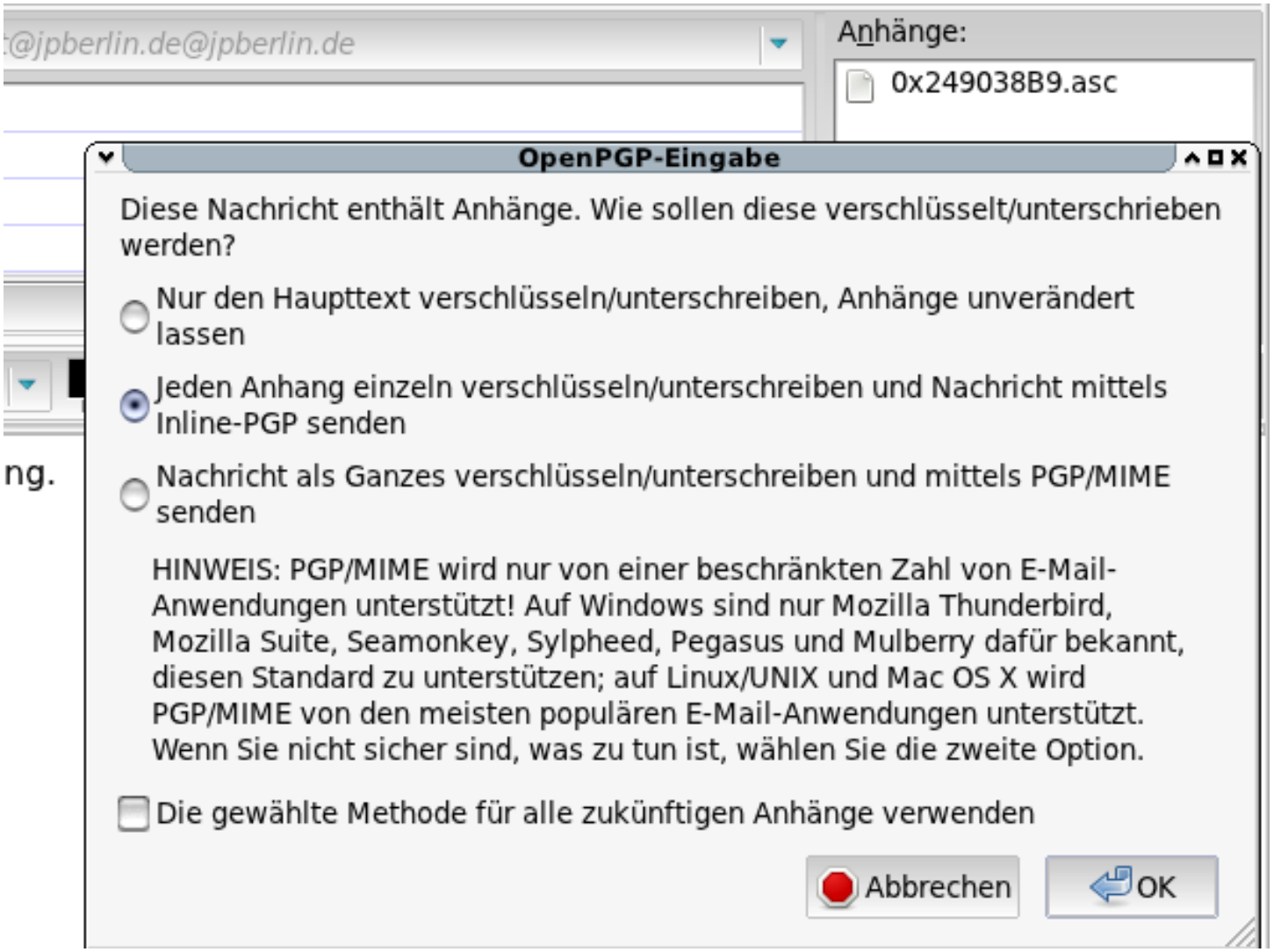

Datei Bearbeiten Ansicht Einfügen Format Einstellungen OpenPGP Extras Hilfe
Senden
Rechtschr.
Anhang
OpenPGP
S/MIME
Speichern

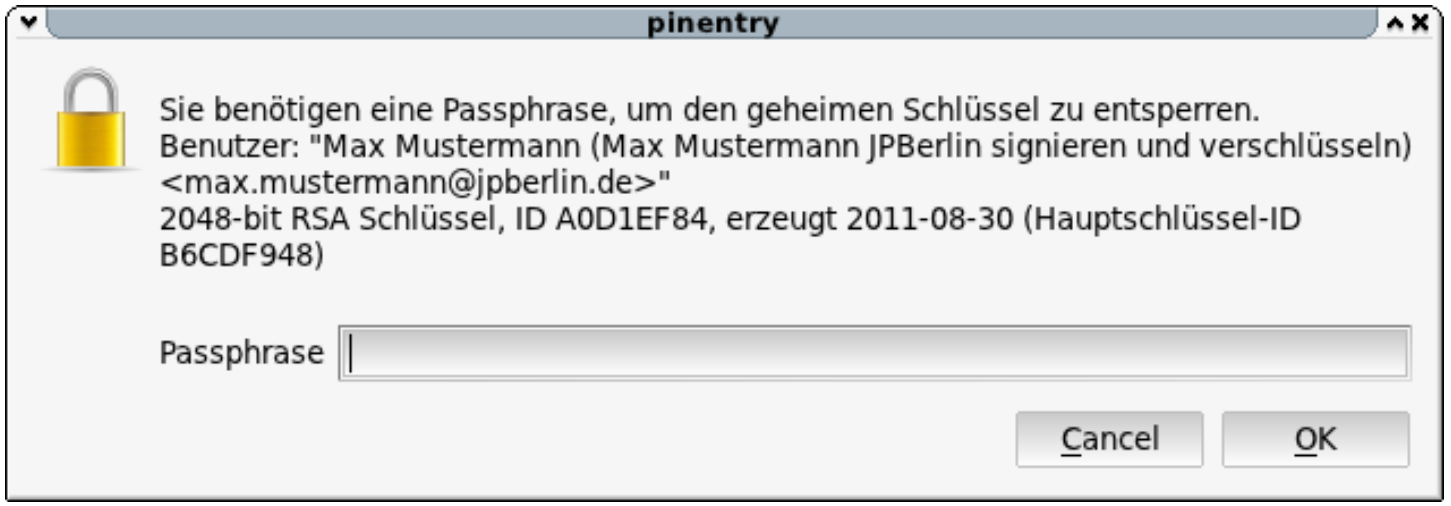

OpenPGP-Sicherheit
Identität: Max Mustermann <max.mustermann@jpberlin.de>
OpenPGP-Unterstützung für diese Identität aktivieren
E-Mail-Adresse dieses Kontos verwenden, um OpenPGP-Schlüssel zu identifizieren
Spezielle OpenPGP-Schlüssel-ID verwenden (0x1234ABCD):
0xB6CDF948
Schlüssel auswählen...
Nachrichten Verfassen Standard-Einstellungen
Unverschlüsselte Nachrichten standardmäßig unterschreiben
Verschlüsselte Nachrichten standardmäßig unterschreiben
Nachrichten standardmäßig verschlüsseln
PGP/MIME standardmäßig verwenden
Erweitert ...
Abbrechen
OK


OpenPGP-Schlüssel verwalten
Datei Bearbeiten Anzeigen Schlüssel-Server Erzeugen
Suchen nach:
Alle zeigen
Standardmäßig alle Schlüsse
Name
Schlüss
Schlüssel-Server auswählen
Suche nach Schlüssel
Schlüssel-Server
pool.sks-keyservers.net
Abbrechen
OK


OpenPGP-Schlüssel verwalten
Datei Bearbeiten Anzeigen Schlüssel-Server Erzeugen
Suchen nach: Max Mustermann
Alle zeigen
Standardmäßig alle Schlüssel anzeigen
Name
Schlüssel-ID
Max Mustermann (Max Mustermann JPBerlin signieren und verschlüsseln) <max.mustermann... B6CDF948
Hat keine weiteren Identitäten
Kein Foto verfügbar


OpenPGP-Sendeopti
Nachricht unterschreiben
Nachricht verschlüsseln
PGP/MIME verwenden
Empfängerregeln ignorieren
Abbrechen
OK


@jpberlin.de@jpberlin.de
Anhänge:
0x249038B9.asc
ng.
OpenPGP-Eingabe
Diese Nachricht enthält Anhänge. Wie sollen diese verschlüsselt/unterschrieben werden?
Nur den Haupttext verschlüsseln/unterschreiben, Anhänge unverändert lassen
Jeden Anhang einzeln verschlüsseln/unterschreiben und Nachricht mittels Inline-PGP senden
Nachricht als Ganzes verschlüsseln/unterschreiben und mittels PGP/MIME senden
HINWEIS: PGP/MIME wird nur von einer beschränkten Zahl von E-Mail-Anwendungen unterstützt! Auf Windows sind nur Mozilla Thunderbird, Mozilla Suite, Seamonkey, Sylpheed, Pegasus und Mulberry dafür bekannt, diesen Standard zu unterstützen; auf Linux/UNIX und Mac OS X wird PGP/MIME von den meisten populären E-Mail-Anwendungen unterstützt. Wenn Sie nicht sicher sind, was zu tun ist, wählen Sie die zweite Option.
Die gewählte Methode für alle zukünftigen Anhänge verwenden
Abbrechen
OK


pinentry
Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Max Mustermann (Max Mustermann JPBerlin signieren und verschlüsseln)
<max.mustermann@jpberlin.de>"
2048-bit RSA Schlüssel, ID A0D1EF84, erzeugt 2011-08-30 (Hauptschlüssel-ID
B6CDF948)
Passphrase
Cancel
OK

Und unser Fazit?

- E-mail-Verschlüsselung einzurichten ist nicht schwer
  - Software installieren
  - Schlüssel generieren
  - Schlüssel veröffentlichen / an Partner per Mail senden
  - Weitermachen wie bisher :-)
- Verzichten Sie auf irgendwelche komischen Lösungen. Nutzen Sie PGP oder S/MIME.

Übrigens...

Ein guter Provider kümmert sich darum Sie und Ihre Daten zu beschützen:

- Gute Provider stehen Ihnen mit Rat und Tat zur Seite
- Gute Provider publizieren Anleitungen
- Gute Provider setzen Verschlüsselung durch
- http://www.jpberlin.de/hilfe

Werfen Sie mal einen Blick auf http://www.jpberlin.de. Wenn Sie auf der Suche nach einem neuen Provider sind, sprechen wir uns vielleicht mal wieder...

JPBERLIN
POLITISCHER PROVIDER

Das sichere E-Mail-Postfach für 1 €/Monat

Die JPBerlin bietet seit 1989 unabhängige und werbefreie E-Mail-Postfächer mit Sitz in Deutschland.

- ✔ Das sichere E-Mail-Postfach für Privat & Business
- ✔ Durchgehende Verschlüsselung mit SSL/TLS
- ✔ Grünes Hosting mit Ökostrom
- ✔ Komplett werbefrei ohne Auswertung von Nutzerdaten
- ✔ Zuverlässiger SPAM-und Virenschutz
- ✔ 1 Mailadresse, 1 GB-Postfach für 1 EUR/Monat
- ✔ Auch große Postfächer > 10 Gbyte buchbar
- ✔ Serverseitige Mailfilterung mit Sieve
- ✔ Mobiler Zugriff über unsere Webmailer
- ✔ Serverstandort Deutschland (Berlin)
- ✔ Deutsches Datenschutzrecht

Extras sind schon inklusive

Mit unserem Sieve-Filter können Sie Ihre E-Mails bereits auf dem Mailserver bearbeiten lassen. Dadurch schaffen Sie Ordnung in Ihrem Postfach und können flexibel reagieren – auch ganz ohne Computer.

Vielen Dank für die Aufmerksamkeit!

Gerne stehe ich Ihnen jetzt und im Anschluß
für Fragen zur Verfügung.