

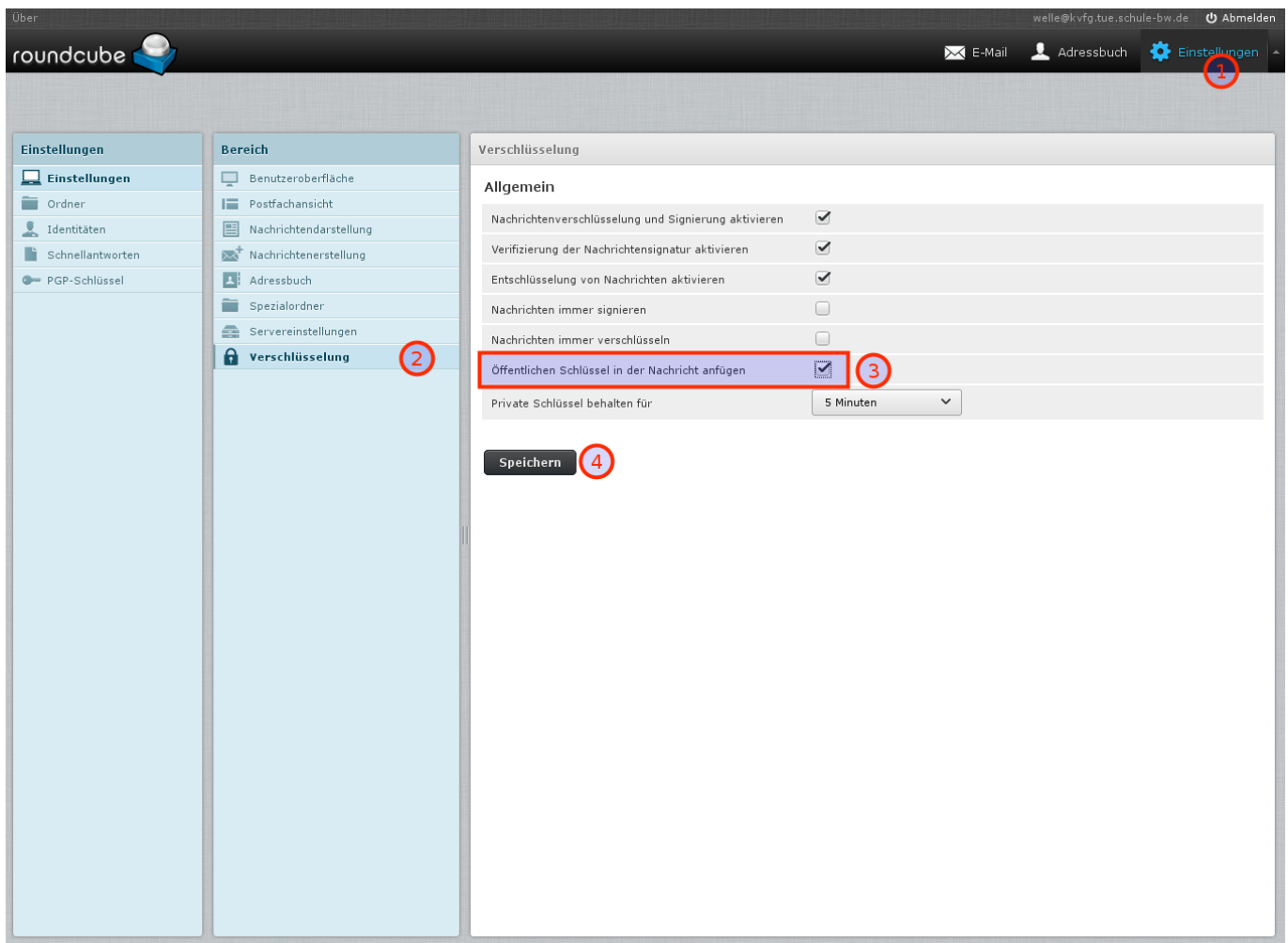
PGP Verschlüsselung für Schüler/innen

Die folgende Anleitung beschreibt, wie Ihr Euch einen PGP-Schlüssel für Euer Konto auf ServerG erstellt und gibt ein paar Hinweise zum Schlüsselmanagement allgemein. Eine Einführung in die Mailverschlüsselung mit PGP / GnuPG erhaltet Ihr hier nicht (zu lang, zu komplex), lediglich noch den (dringenden) Hinweis auf [diese Seiten zur Lektüre](#).

Schlüsselerstellung

Meldet Euch am Webmailer für Euer Konto `benutzername@kvfg.tue.schule-bw.de` an:

<https://kvfg.eu/webmail/>



Klickt dann auf

- Einstellungen
- Verschlüsselung
- Öffentlichen Schlüssel in der Nachricht anfügen
- Speichern

Diese Schritte sorgen dafür, dass alle Eure E-Mail-Empfänger in Zukunft Euren öffentlichen Schlüssel

mit Eurer Mail zusammen erhalten. Das ist die Voraussetzung, um Euch später einmal verschlüsselt schreiben zu können.

roundcube

Über welle@kvfg.tue.schule-bw.de Abmelden

E-Mail Adressbuch Einstellungen

Importieren Exportieren

Einstellungen

- Einstellungen
- Ordner
- Identitäten
- Schnellantworten
- PGP-Schlüssel

PGP-Schlüssel

Neues Schlüsselpaar erstellen

Identität: Dirk Weller <welle@kvfg.tue.schule-bw.de>

Schlüssellänge: 4096 Bit - mehr Sicherheit

Passwort:

Passwort bestätigen:

Speichern

Keine Schlüssel gefunden

Im nächsten Schritt erzeugt Ihr Euer Schlüsselpaar. „Paar“, weil es sich um zwei miteinander mathematisch verbundene Schlüssel handelt: einen öffentlichen (zum Weitergeben) und einen privaten oder geheimen (den Ihr nie weitergeben dürft).

Klickt also auf

- PGP-Schlüssel
- (+)
- stellt die Schlüsselstärke ein
- vergibt ein richtig gutes und langes Passwort ohne Umlaute, Leerzeichen oder Ligaturen (wie „ß“ usw)
- schreibt Euch dieses Passwort auf!
- klickt auf Speichern

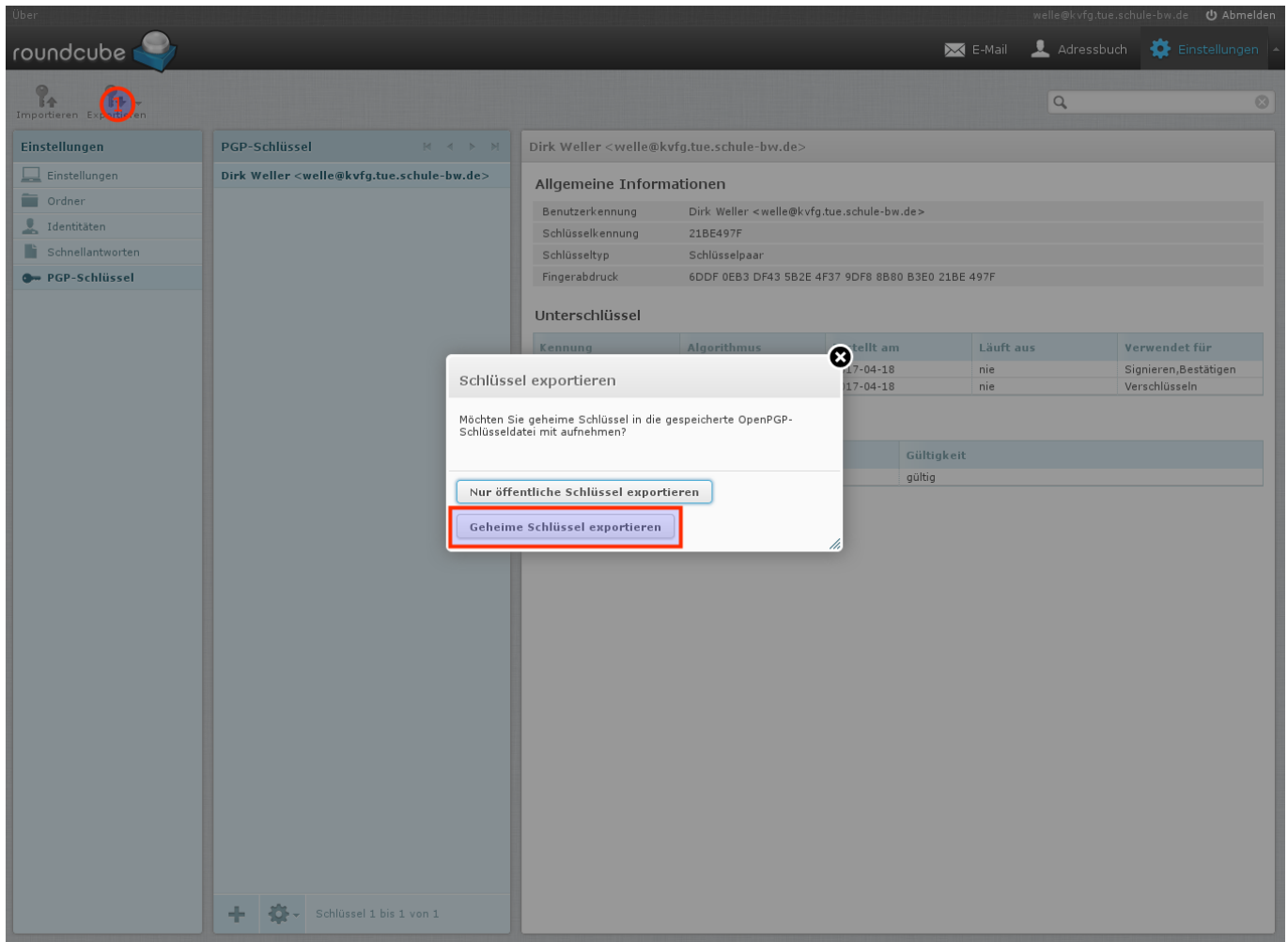
Dann müsst Ihr warten, bis der Server genug Zufall gesammelt hat, um Euren Schlüssel zu backen. Das kann dauern.



Solltest Du Dein Schlüsselpasswort vergessen, dann gibt es keine Möglichkeit, dieses wiederherzustellen!



Solltest Du Deine Schlüssel verlieren, dann gibt es keine Möglichkeit, diese wiederherzustellen!



Dein Schlüsselbund liegt nun auf unserem Server, ist aber nur durch das Passwort geschützt, das Du diesem gegeben hast. Zur Sicherheit (z.B. falls der Server mal über die Wupper geht) solltest Du Dir Deinen Schlüsselbund herunterladen. Dazu klickst Du

- auf Exportieren
- Geheime Schlüssel exportieren

und speicherst die Datei lokal so weg, dass außer Dir keiner da dran kommt. Ein VeraCrypt-Container ist eine gute Wahl!

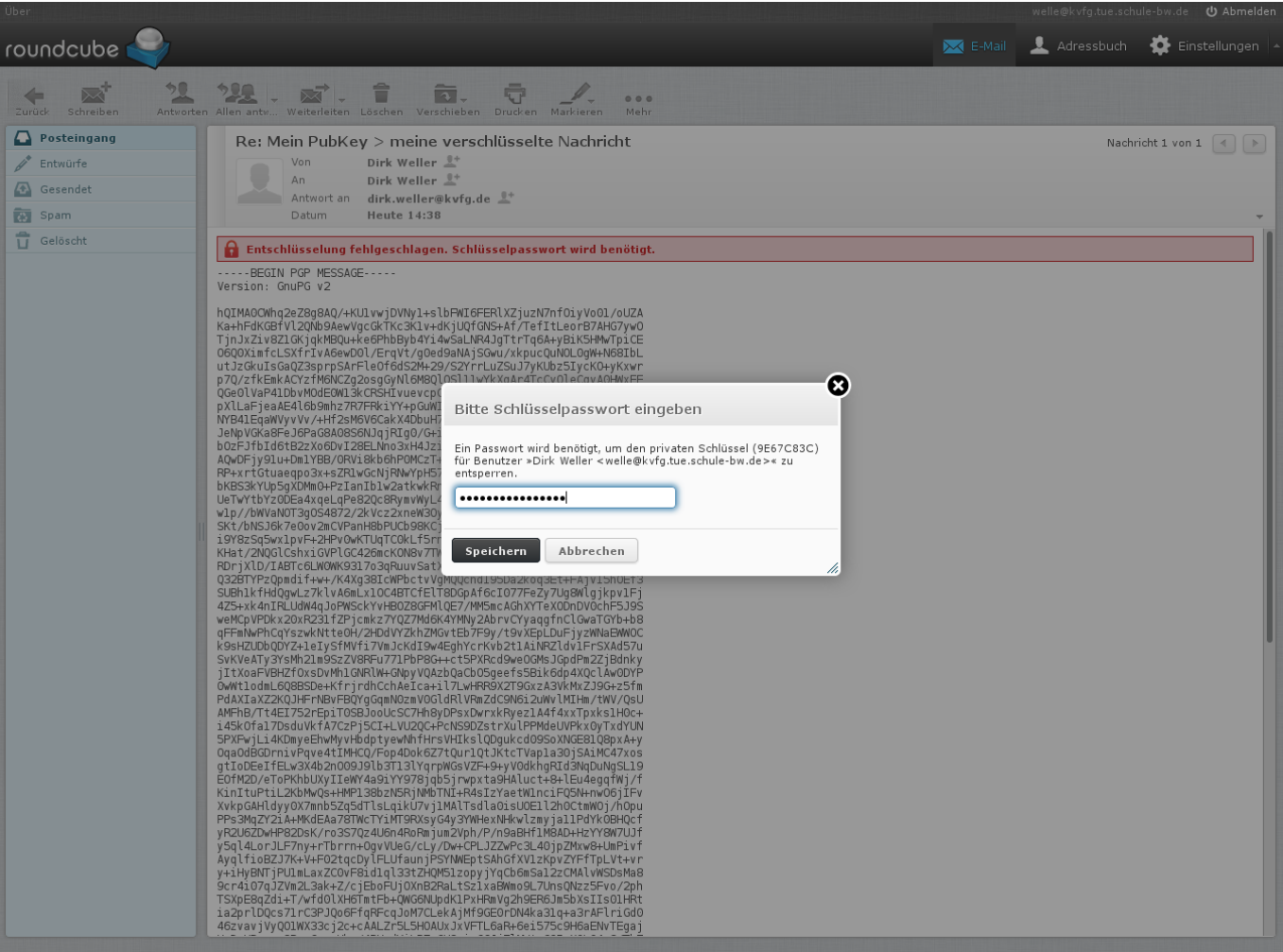


Kein Backup? Kein Mitleid!

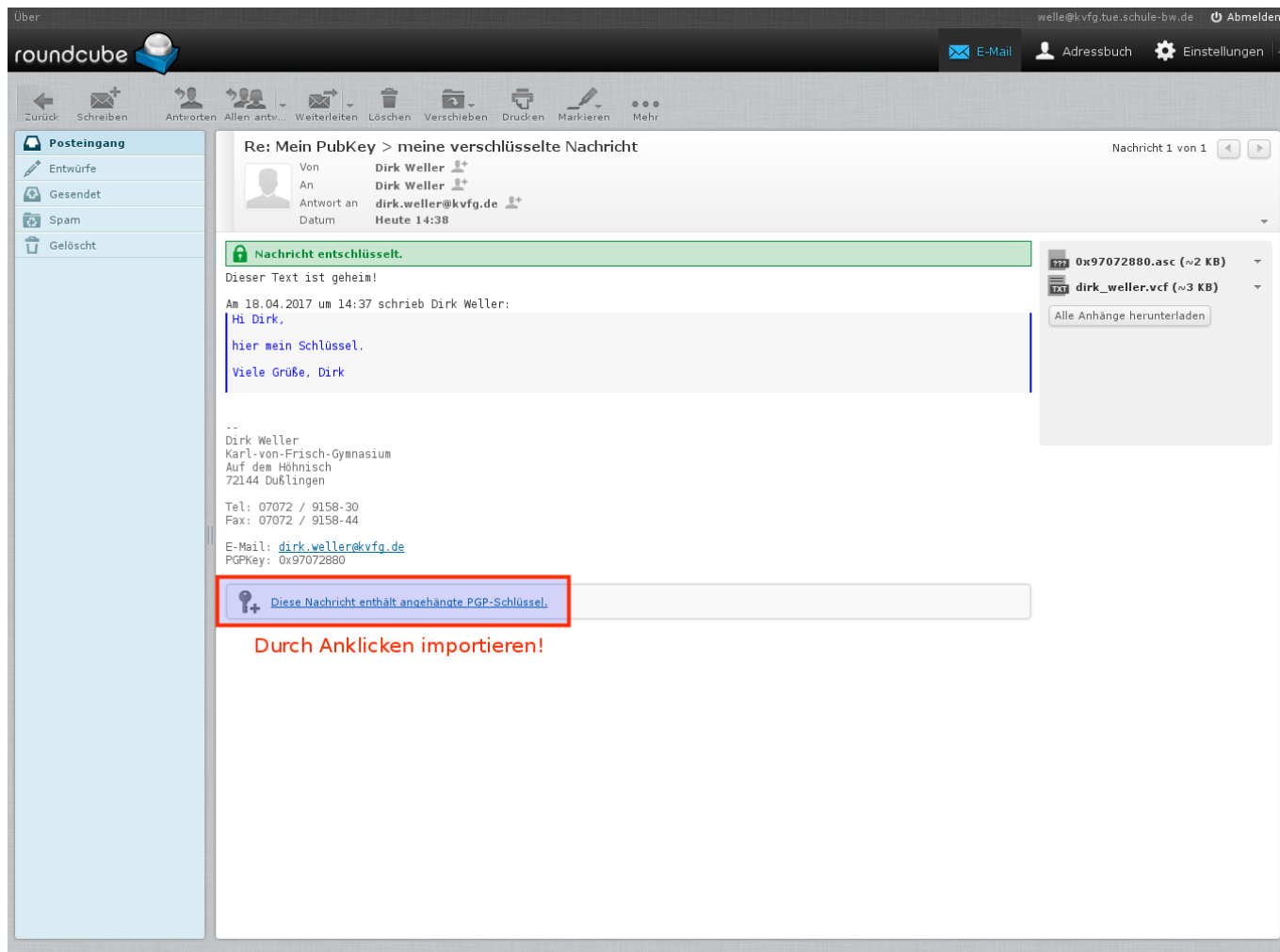
Entschlüsseln

Du verschickst, sofern Du die Anleitung oben befolgt hast, nun E-Mails mit Deinem öffentlichen Schlüssel im Anhang. Jeder, der PGP verwendet, kann Dir nun verschlüsselte Nachrichten zukommen lassen, nachdem er / sie Deinen öffentlichen Schlüssel in das eigene Mailprogramm importiert hat.

Das sieht dann bei Dir so aus:



Im Hintergrund siehst Du die E-Mail wie die NSA diese sieht 😊 - totales Zeichenwirrwar. Im Vordergrund ploppt ein Fensterchen auf, in dem Du nach Deinem Schlüsselpasswort gefragt wirst. Gib dieses ein und klick auf Speichern. Roundcube merkt sich Dein Schlüsselpasswort für ca. 5 Minuten.



Jetzt kannst Du die Mail im entschlüsselten Klartext lesen.

Schlüsselmanagement

Unten an den LuL-Mails siehst Du deren öffentlichen Schlüssel angehängt (siehe Bild oben). Klick auf diesen Schlüssel (für jeden Lehrer neu), um diesen in Deinen Schlüsselspeicher zu importieren.

Dann kannst Du den LuL, von denen Du die öffentlichen Schlüssel hast, verschlüsselte Nachrichten zukommen lassen!

The screenshot shows the Roundcube webmail interface. On the left, the 'Einstellungen' (Settings) menu is open, with 'PGP-Schlüssel' (PGP Keys) selected. The main content area displays the details for a PGP key. The key is titled 'Dirk Weller <dirk.weller@kvfg.de>' and is associated with the email address 'Dirk Weller <welle@kvfg.tue.schule-bw.de>'. The key's fingerprint is 9D09 A21A FAA6 362C 4378 8840 5778 ADF2 9707 2880. The key is an RSA (2048) key, created on 2014-08-30, and is currently valid. The key is used for signing and encryption.

PGP-Schlüssel

Dirk Weller <dirk.weller@kvfg.de>

Dirk Weller <welle@kvfg.tue.schule-bw.de>

Allgemeine Informationen

Benutzerkennung	Dirk Weller <dirk.weller@kvfg.de>
Schlüsselkennung	97072880
Schlüsseltyp	Öffentlicher Schlüssel
Fingerabdruck	9D09 A21A FAA6 362C 4378 8840 5778 ADF2 9707 2880

Unterschlüssel

Kennung	Algorithmus	Erstellt am	Läuft aus	Verwendet für
97072880	RSA (2048)	2014-08-30	nie	Verschlüsseln, Signiere...
EF839B56	RSA (2048)	2014-08-30	nie	Verschlüsseln, Signiere...

Zusätzliche Benutzer

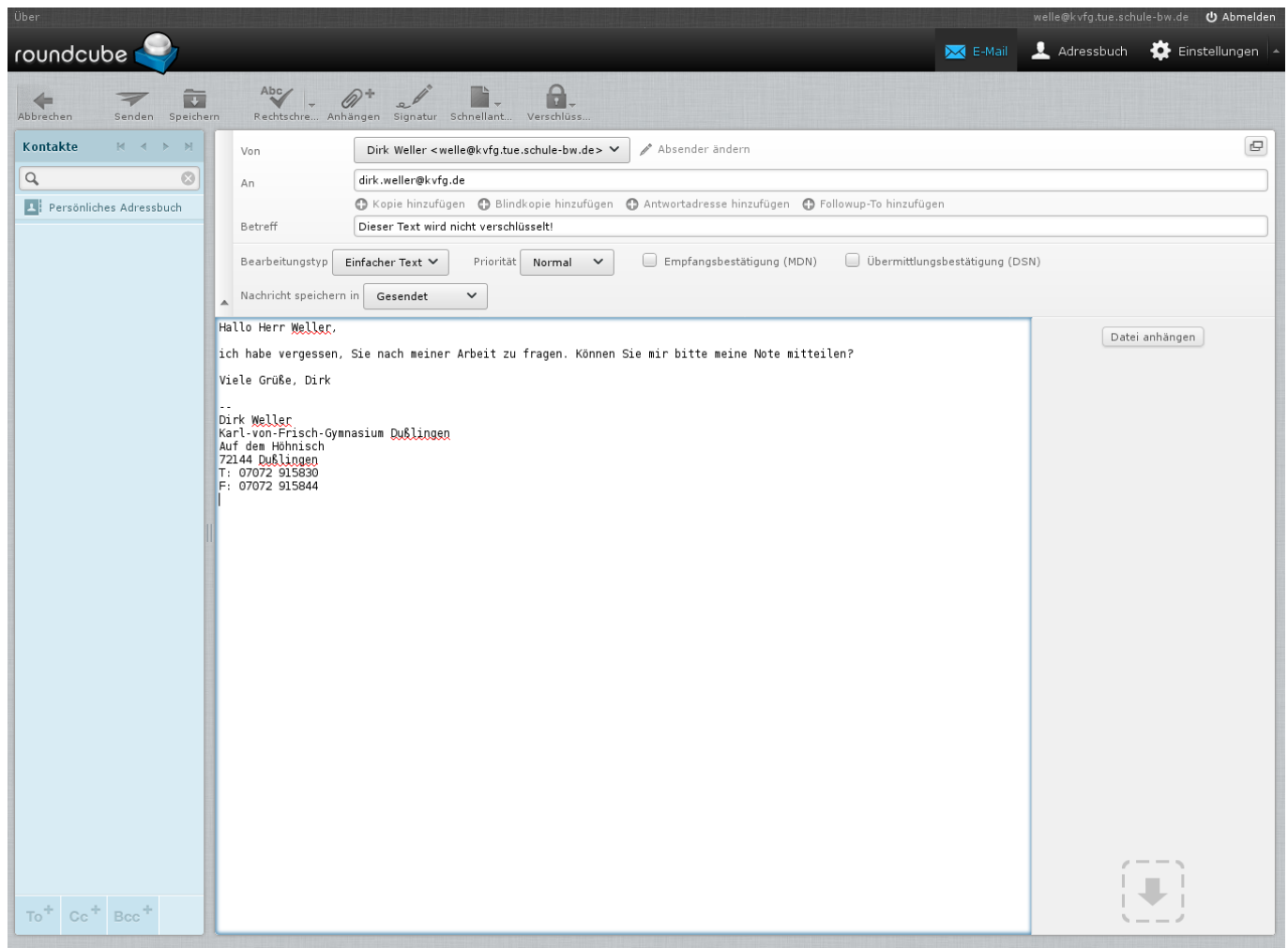
Kennung	Gültigkeit
Dirk Weller <dirk.weller@kvfg.de>	gültig

Wenn Du die von Dir bereits eingesammelten Schlüssel ansehen willst, dann klick auf

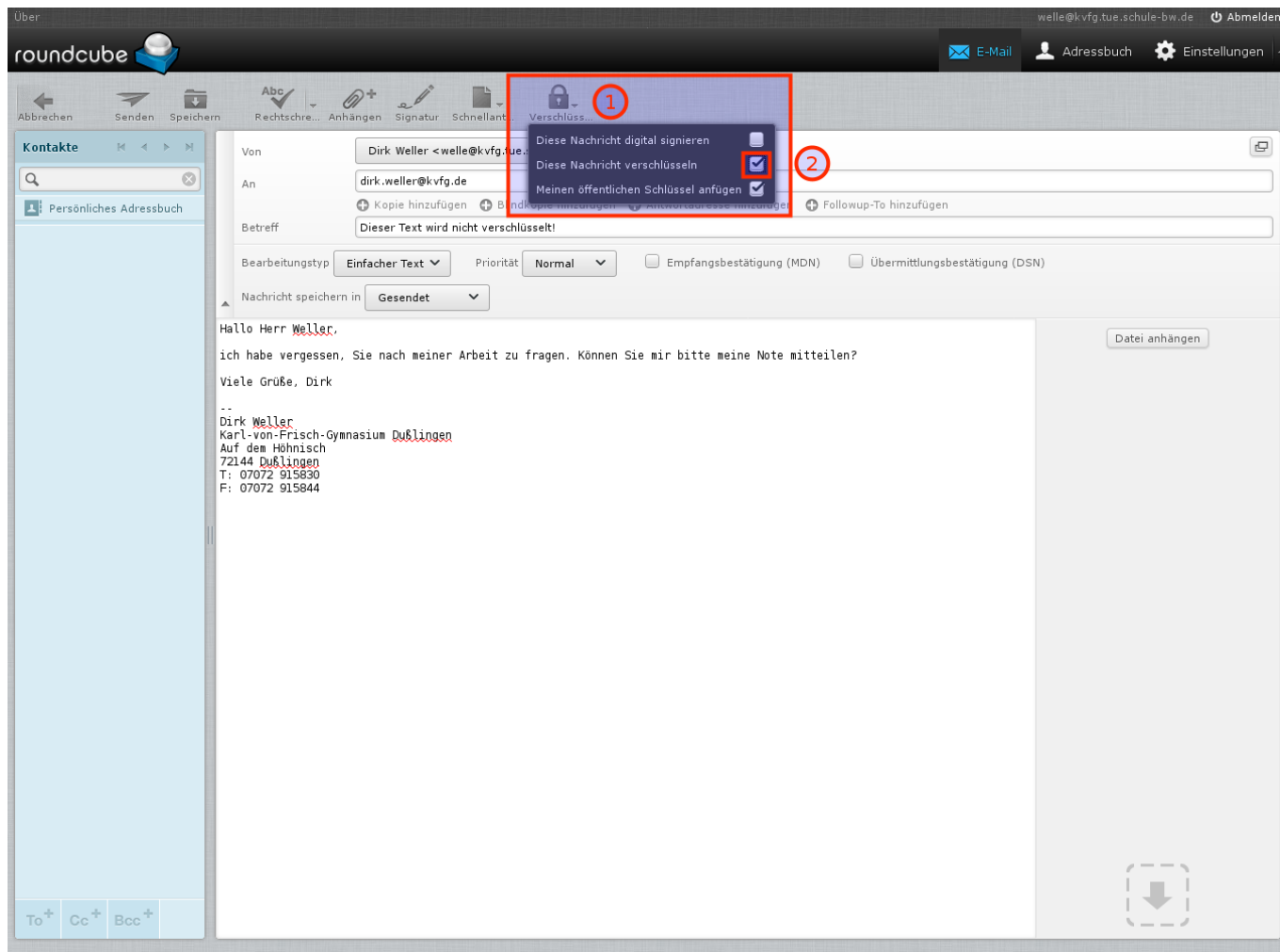
- Einstellungen
- PGP-Schlüssel

Dort kannst Du die Schlüssel verwalten - z.B. exportieren (oder andere Schlüssel importieren).

Mail verschlüsseln



Schreibe „ganz normal“ Deine Nachricht an die Lehrkraft. Du musst Dir zu diesem Zeitpunkt lediglich im Klaren sein, dass die Betreffzeile nicht verschlüsselt werden kann. Also schreib da nix Wichtiges rein!



Wenn Du Deine Mail fertig formuliert hast, dann klickst Du auf

- Verschlüsselungsoptionen
- Diese Nachricht verschlüsseln
- Senden

Fertig.

Jetzt heißt es Hoffen, dass die Lehrkraft, die Deine verschlüsselte Mail erhalten hat, Dir auch verschlüsselt antwortet und nicht die ganze Mühe durch totale Trotteligkeit wieder zunichte macht, weil sie Dir unverschlüsselt zurückschreibt.

From:
<https://www.kvfg.net/wiki/> - **KvFG Wiki**

Permanent link:
<https://www.kvfg.net/wiki/doku.php?id=netz:pgp4sus&rev=1492524128>

Last update: **2017/04/18 16:02**

