

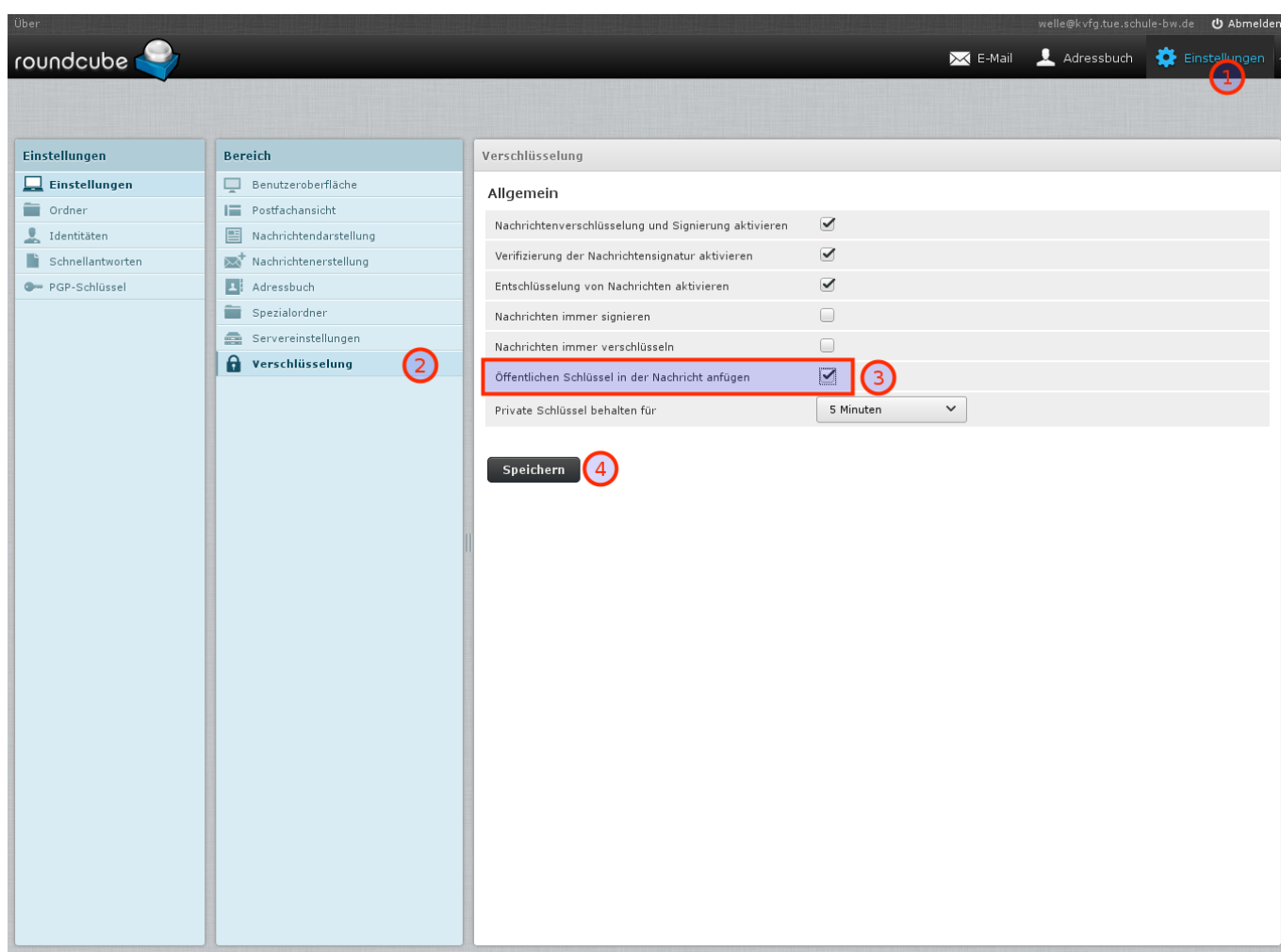
PGP Verschlüsselung für Schüler/innen

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.

The screenshot shows the Roundcube webmail interface. The left sidebar has a menu with 'Einstellungen' (Settings) selected, and 'PGP-Schlüssel' (PGP Key) is highlighted. The main area is divided into two panels: 'PGP-Schlüssel' on the left and 'Neues Schlüsselpaar erstellen' (Create new key pair) on the right. The 'PGP-Schlüssel' panel shows 'Keine Schlüssel gefunden' (No keys found). The 'Neues Schlüsselpaar erstellen' panel has a form with the following fields: 'Identität:' (Identity) with a dropdown menu showing 'Dirk Weller <welle@kvfg.tue.schule-bw.de>', 'Schlüssellänge:' (Key length) with a dropdown menu showing '4096 Bit - mehr Sicherheit', 'Passwort:' (Password) with a text input field, and 'Passwort bestätigen:' (Confirm password) with a text input field. There is a 'Speichern' (Save) button at the bottom of the form. Red circles with numbers 1 through 4 are overlaid on the interface to indicate the steps: 1. Click the '+' button in the PGP-Schlüssel panel. 2. Select the key length (4096 Bit - mehr Sicherheit). 3. Enter a password. 4. Click the 'Speichern' (Save) button.

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 (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

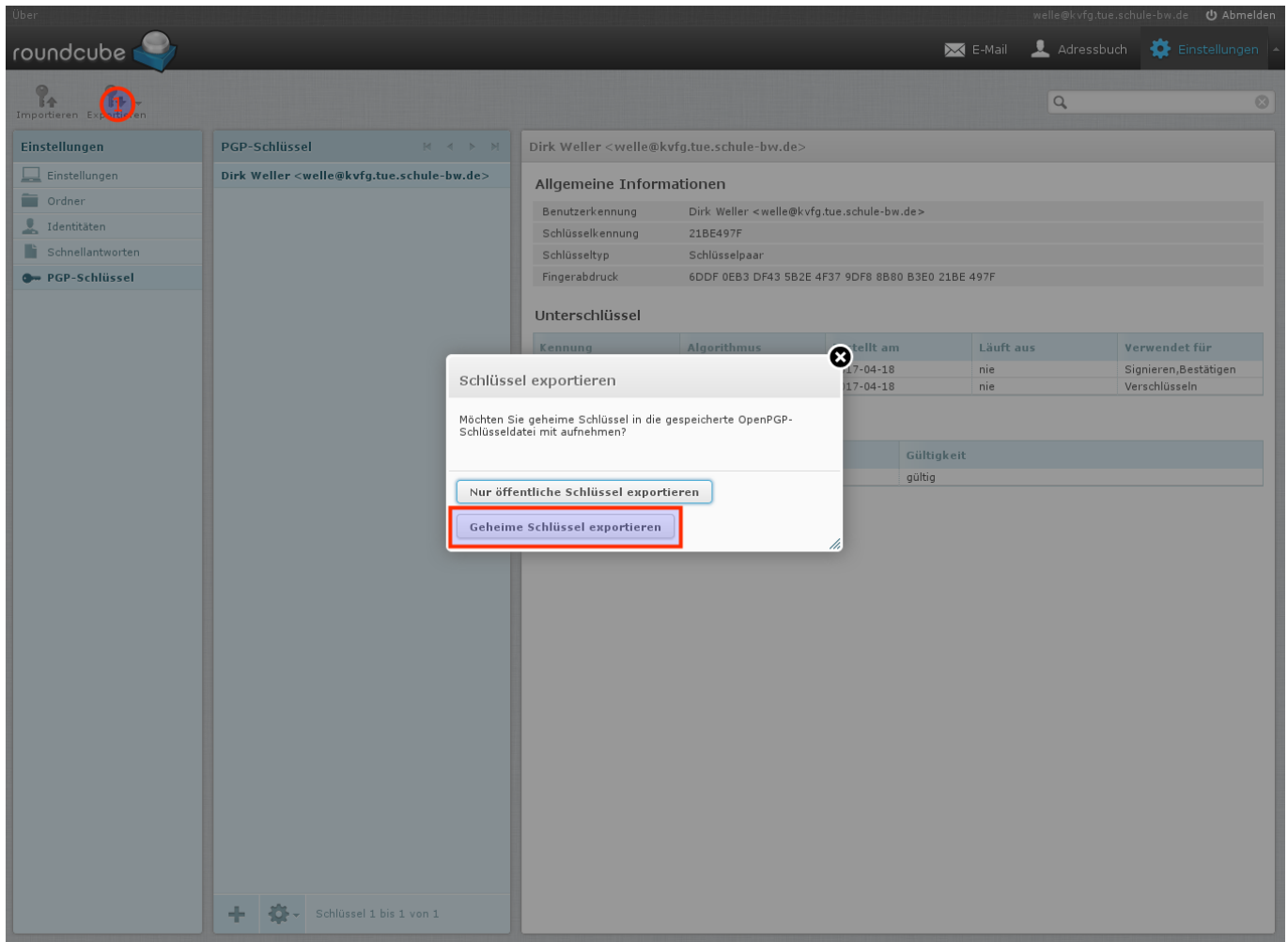
Dann müsst Ihr warten, bis der Server genug Zufall gesammelt hat, um Euren Schlüssel zu backen. Das kann dauern.



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



Solltest Du Deinen privaten Schlüssel verlieren, dann gibt es keine Möglichkeit, diesen wiederherzustellen!



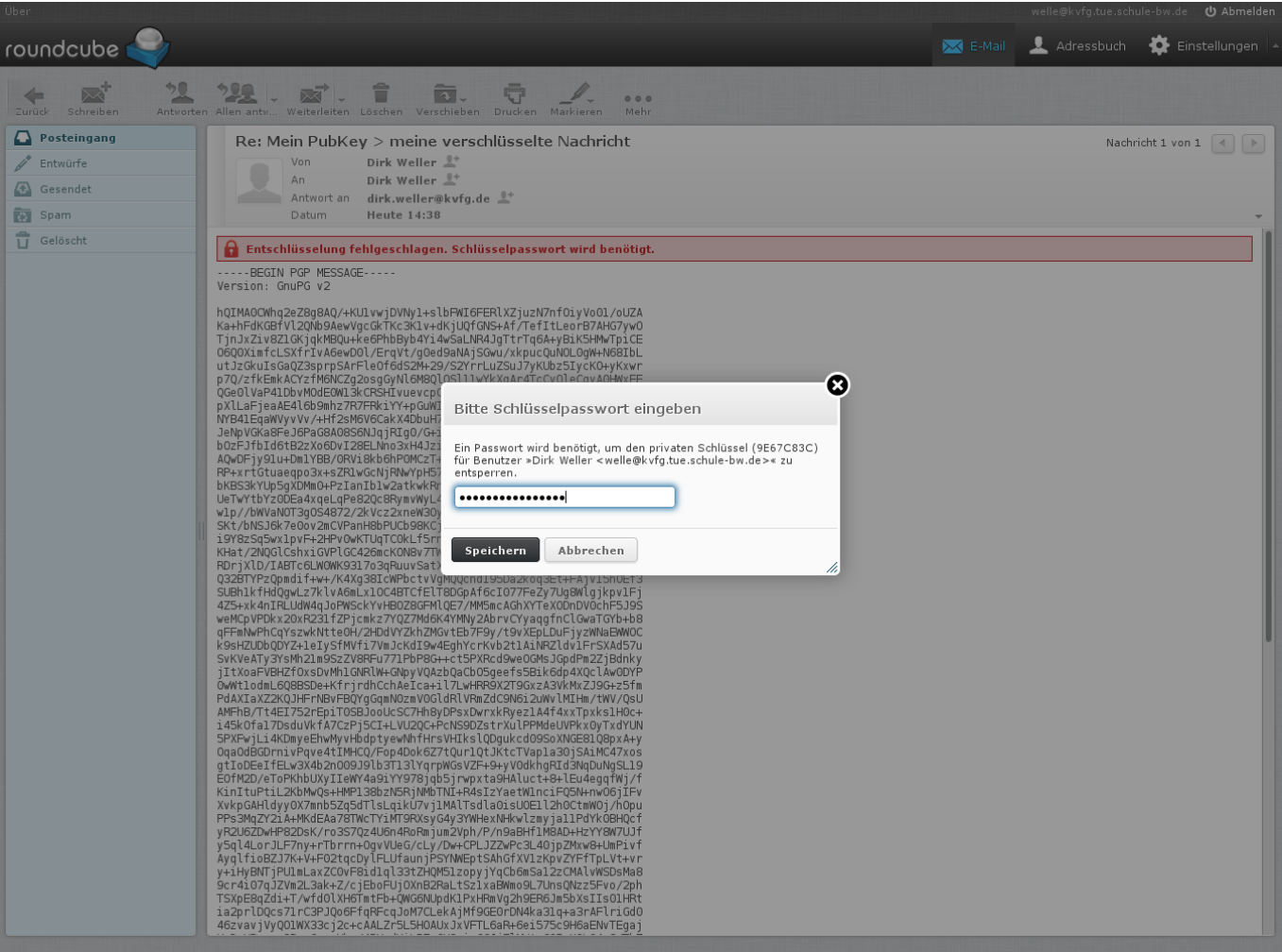
Dein Schlüsselbund liegt nun auf unserem Server und ist nur durch das Passwort geschützt, das Du diesem gegeben hast. Zur Sicherheit (z.B. falls der Server mal über die Wupper geht) solltest Du Dir Deinen Schlüsselbund herunterladen. Dazu klickst Du

- auf Exportieren
- Geheime Schlüssel exportieren

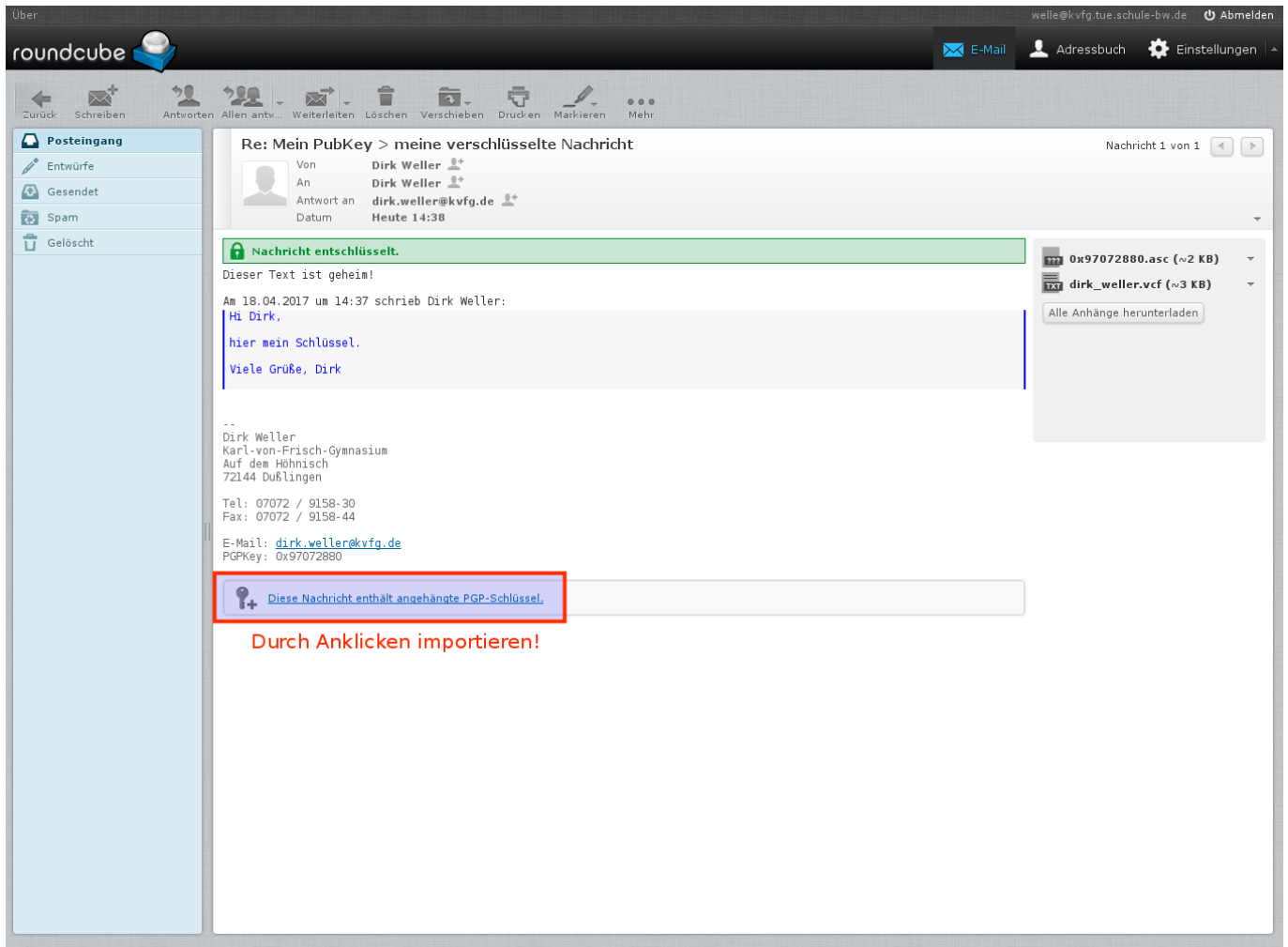
und speicherst die Datei lokal so weg, dass außer Dir keiner da dran kommt. Ein VeraCrypt-Container ist eine gute Wahl!

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 😊). 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 Mails von den LuL 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 verschlüsselte Nachrichten zukommen lassen!

The screenshot shows the Roundcube webmail interface. On the left, a sidebar menu under 'Einstellungen' (Settings) includes 'Einstellungen', 'Ordner', 'Identitäten', 'Schnellantworten', and 'PGP-Schlüssel'. The 'PGP-Schlüssel' option is selected and highlighted with a red box. The main content area displays the PGP key management for 'Dirk Weller <dirk.weller@kvfg.de>'. It includes a section for 'Allgemeine Informationen' (General Information) with fields for 'Benutzerkennung' (User ID), 'Schlüsselkennung' (Key ID), 'Schlüsseltyp' (Key type), and 'Fingerabdruck' (Fingerprint). Below this is a table for 'Unterschlüssel' (Subkeys) with columns for 'Kennung' (ID), 'Algorithmus' (Algorithm), 'Erstellt am' (Created), 'Läuft aus' (Expires), and 'Verwendet für' (Used for). The table shows two subkeys: one for encryption and signing, and another for encryption and signing. At the bottom, there is a section for 'Zusätzliche Benutzer' (Additional users) with a table showing the user 'Dirk Weller <dirk.weller@kvfg.de>' and their status as 'gültig' (valid).

roundcube

Über

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

E-Mail Adressbuch Einstellungen

Importieren Exportieren

Einstellungen

Einstellungen

Ordner

Identitäten

Schnellantworten

PGP-Schlüssel

PGP-Schlüssel

Dirk Weller <dirk.weller@kvfg.de>

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

Dirk Weller <dirk.weller@kvfg.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 |

+

+

Schlüssel 1 bis 2 von 2

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

roundcube

Über E-Mail Adressbuch Einstellungen

Abbrechen Senden Speichern Rechtschre... Anhängen Signatur Schnellant... Verschlüss...

Kontakte

Persönliches Adressbuch

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

An dirk.weller@kvfg.de

Betreff Dieser Text wird nicht verschlüsselt!

Bearbeitungstyp Einfacher Text Priorität Normal

Nachricht speichern in Gesendet

Hallo Herr Weller.

ich habe vergessen, Sie nach meiner Arbeit zu fragen. Können Sie mir bitte meine Note mitteilen?

Viele Grüße, Dirk

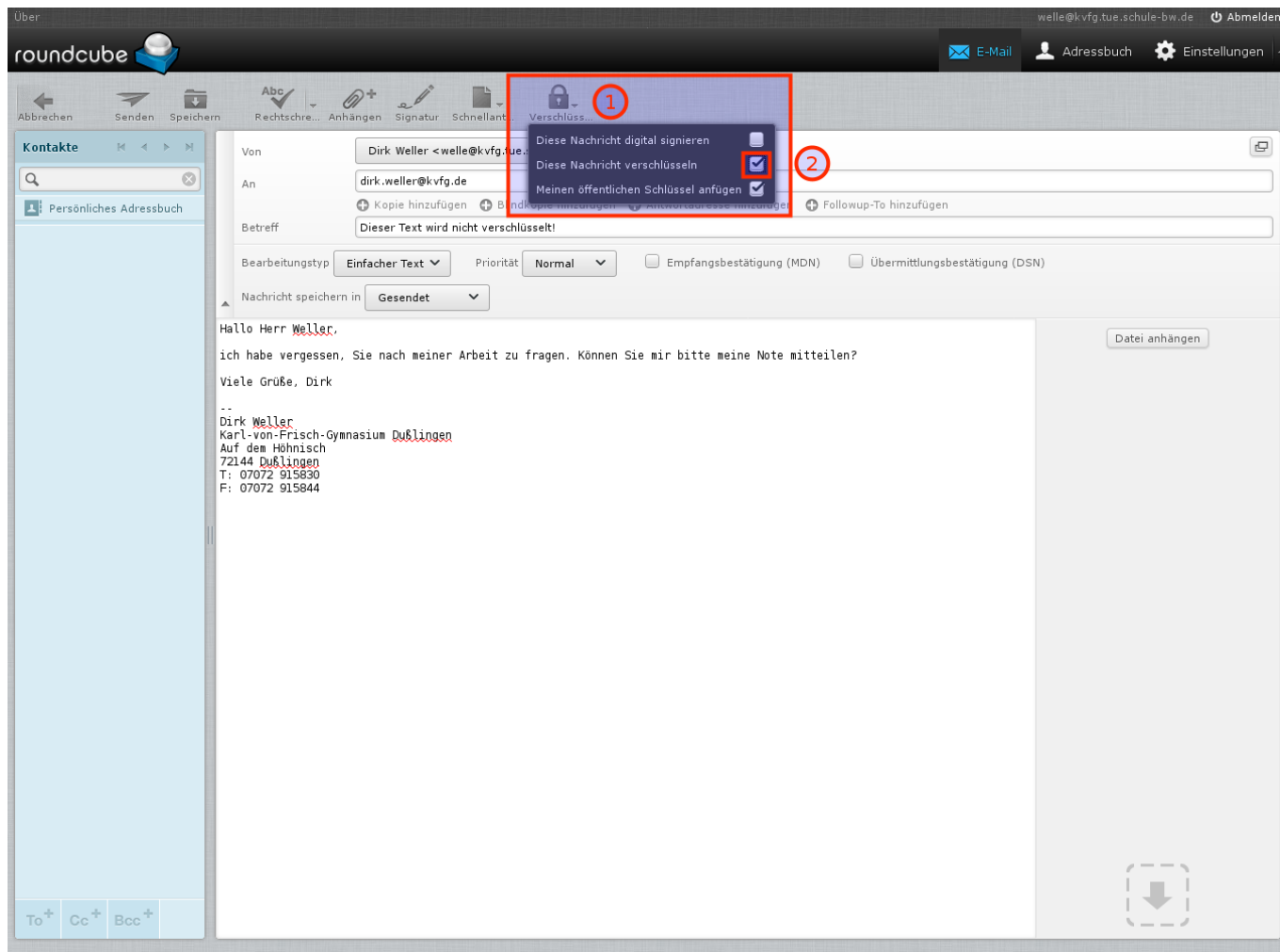
--

Dirk Weller
Karl-von-Frisch-Gymnasium Dußlingen
Auf dem Hühnisch
72144 Dußlingen
T: 07072 915830
F: 07072 915844

Datei anhängen

To+ Cc+ Bcc+

Jetzt schreibst Du „ganz normal“ Deine Nachricht an Deine Lehrkraft. Du musst Dir aber 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
- setzt einen Haken bei Diese Nachricht verschlüsseln
- und klickst auf 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=1492523615>

Last update: **2017/04/18 15:53**

