PGP Verschlüsselung für Schüler/innen

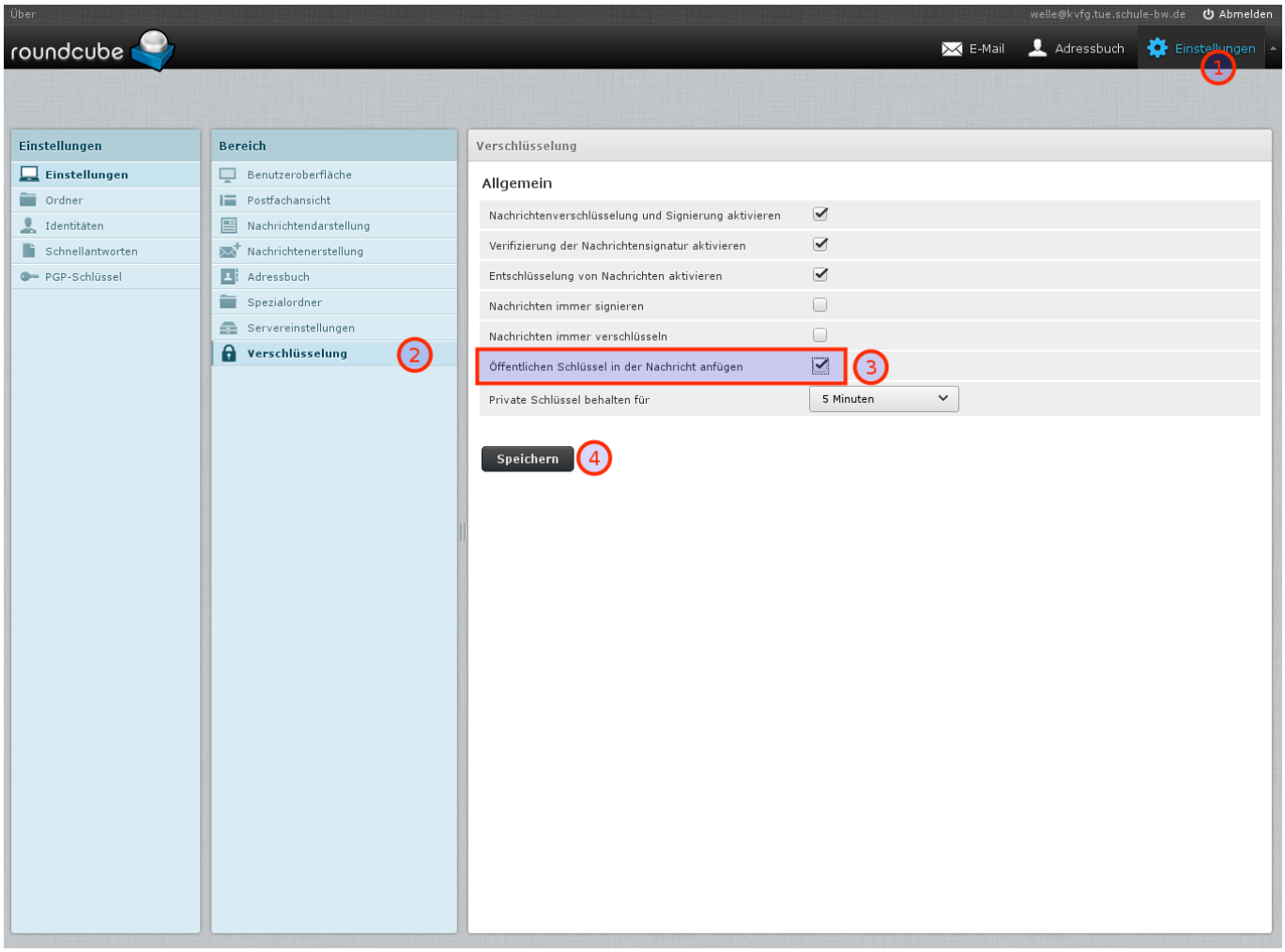
Die folgende Anleitung beschreibt, wie Ihr Euch einen PGP-Schlüssel für Euer Konto auf ServerG erstellt und gibt ein paar Hinweise zum Schlüsselmanagement allgemein. Eine Einführung in die Mailverschlüsselung mit PGP / GnuPG erhaltet Ihr hier nicht (zu lang, zu komplex), lediglich noch den (dringenden)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

01.08.2017: Die Maildomain von ServerG hat sich geändert! Du musst Deinen Schlüssel für benutzer@kvfg.tue.schule-bw.de exportieren und dann in Roundcube löschen. Dann musst Dir für benutzer@kvfg-schule.de einen neuen Schlüssel anlegen!

Schlüsselerstellung

Melde Dich am Webmailer für Dein Konto benutzername@kvfg.tue.schule-bw.de an:

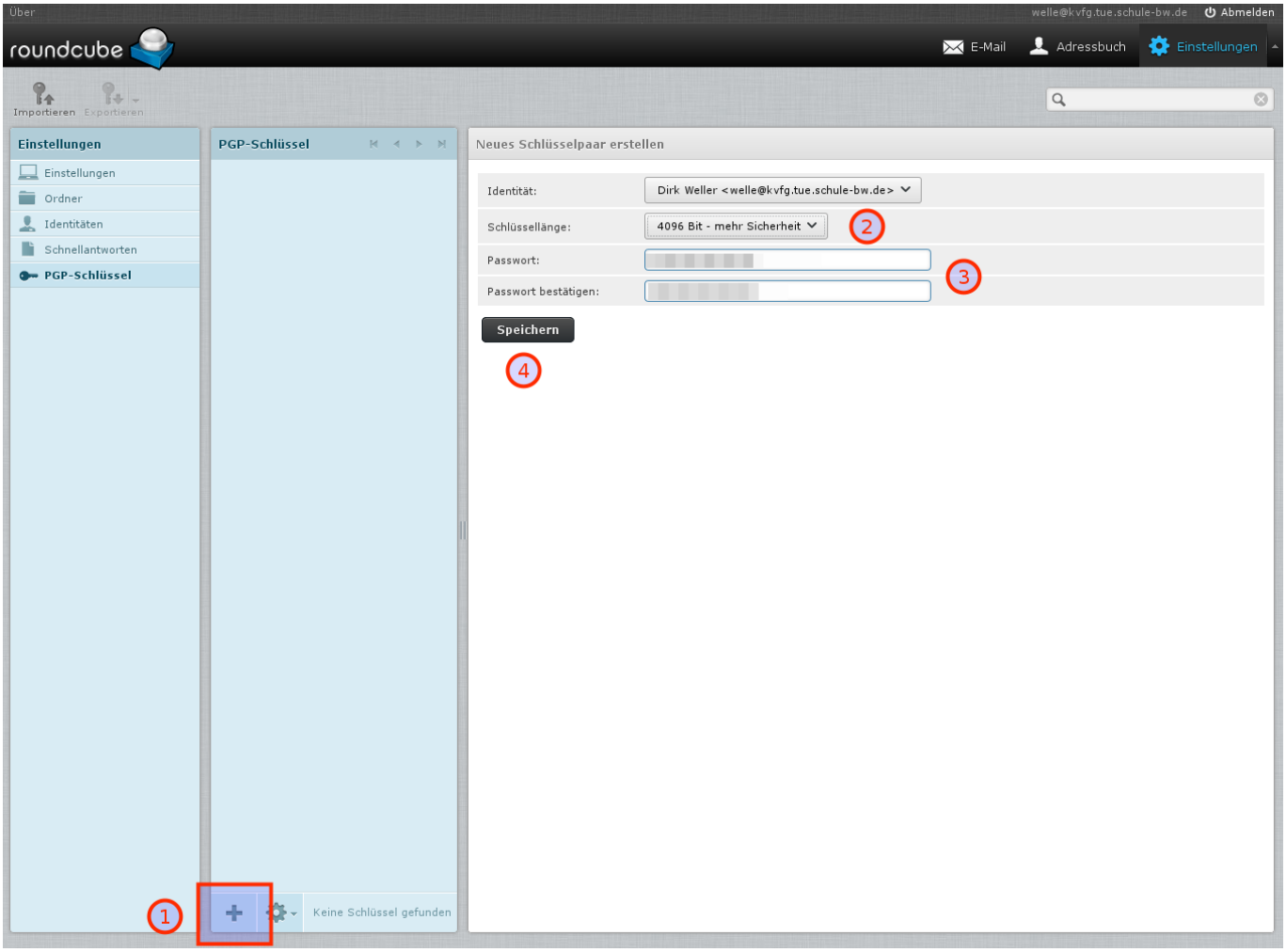
https://kvfg.eu/webmail/



Klick dann auf

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

Diese Schritte sorgen dafür, dass alle Deine E-Mail-Empfänger in Zukunft Deinen öffentlichen Schlüssel mit Deiner Mail zusammen erhalten. Das ist die Voraussetzung, um Dir später einmal verschlüsselt schreiben zu können.



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

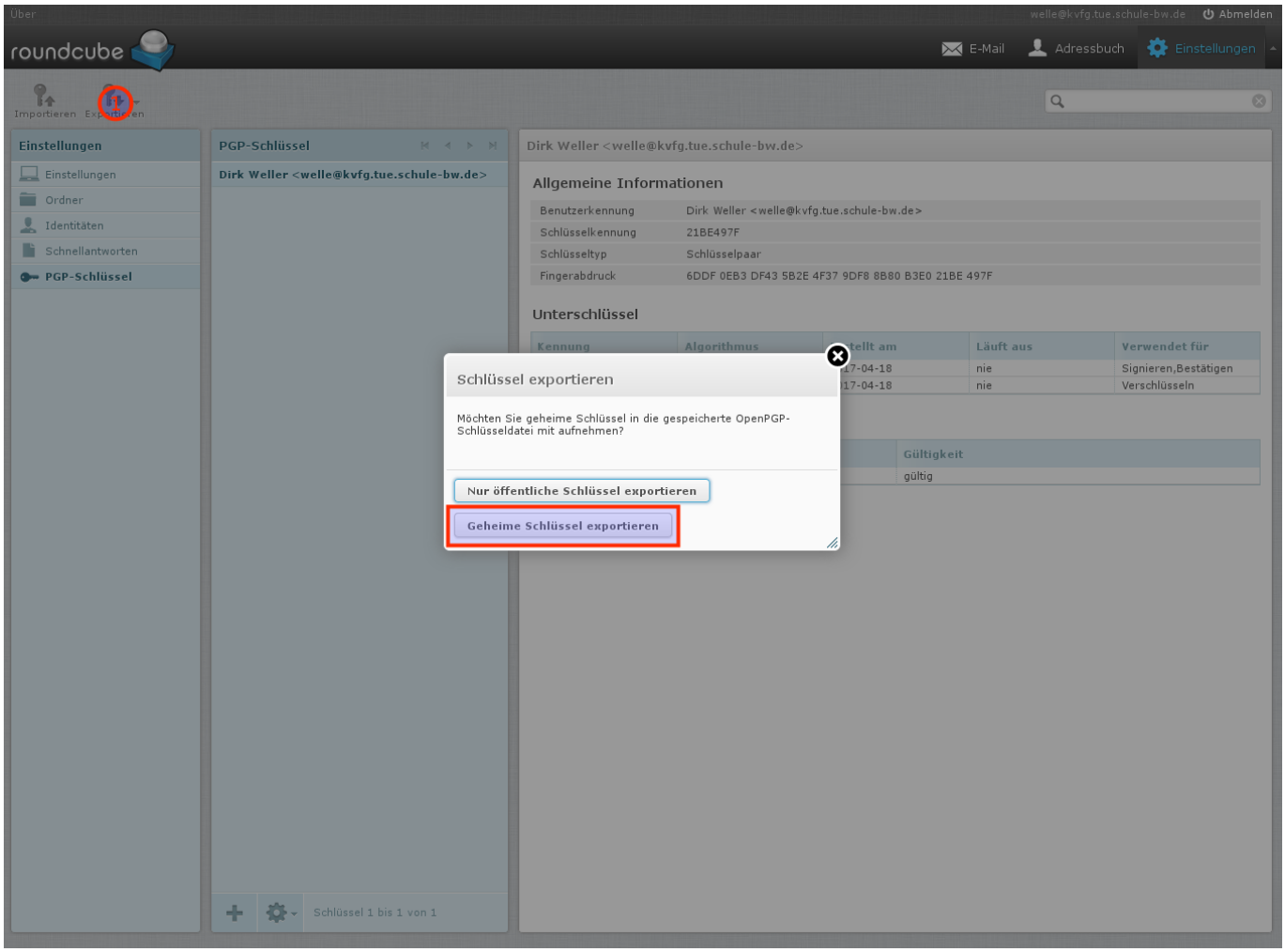
Klick also auf

- PGP-Schlüssel
- (+)
- stelle die Schlüsselstärke ein (2000er reicht)
- vergib ein richtig gutes und langes Passwort ohne Umlaute, Leerzeichen oder Ligaturen (wie „ß“ usw)
- schreib Dir dieses Passwort auf!
- klick auf Speichern

Dann musst Du warten, bis der Server genug Zufall gesammelt hat, um Deine 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

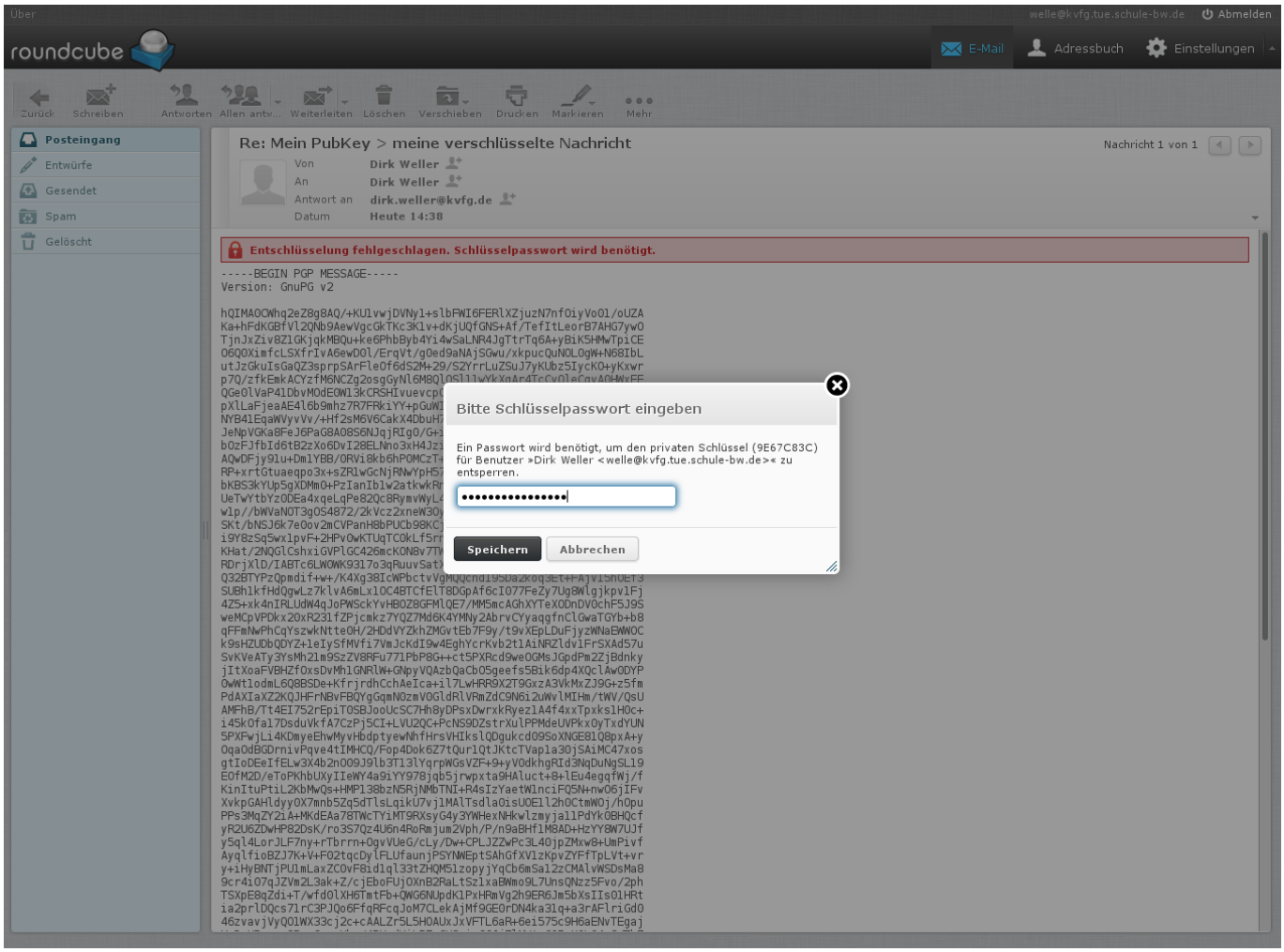
- Exportieren
- Geheime Schlüssel exportieren

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

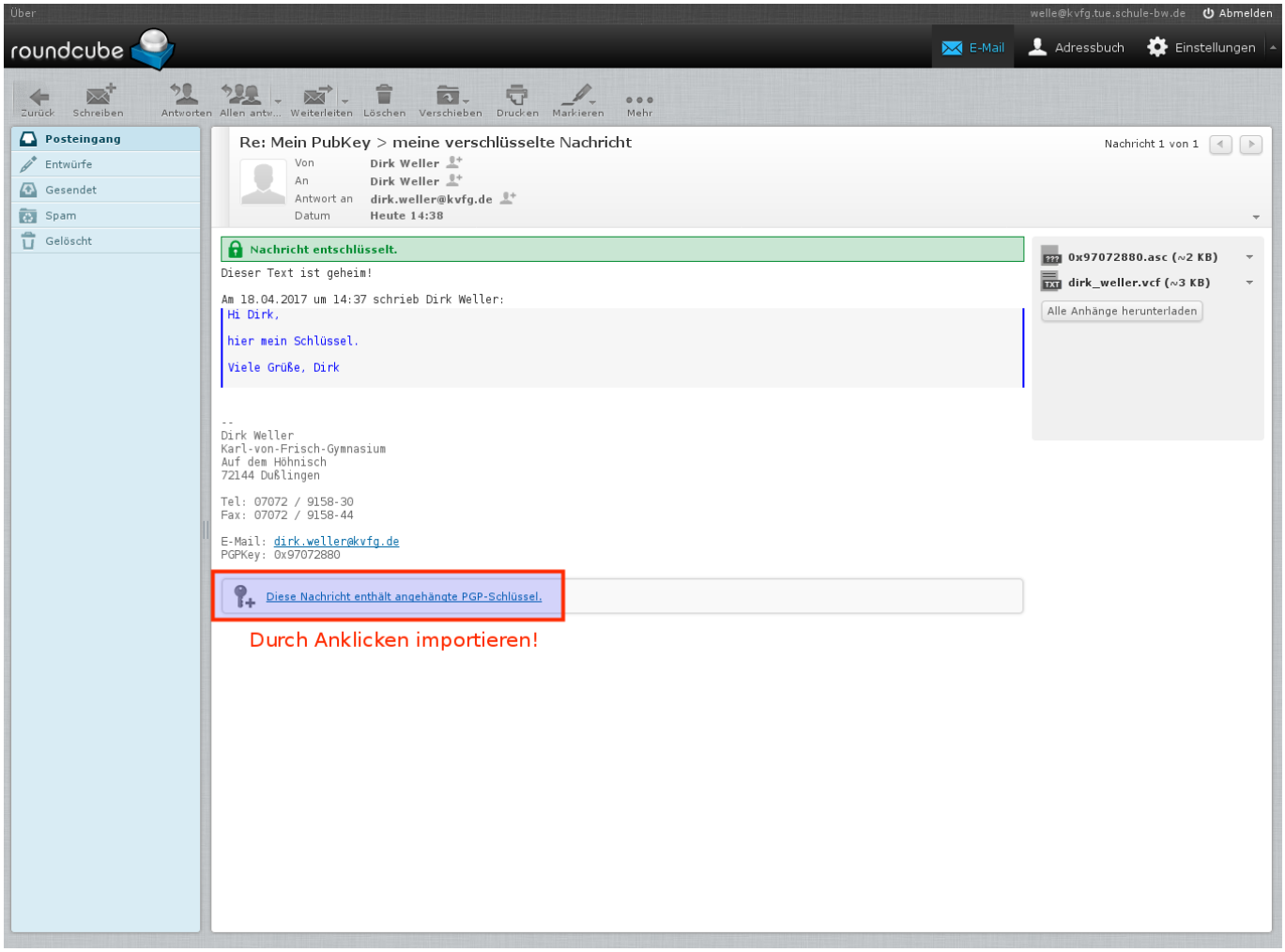
Kein Backup? Kein Mitleid!

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.

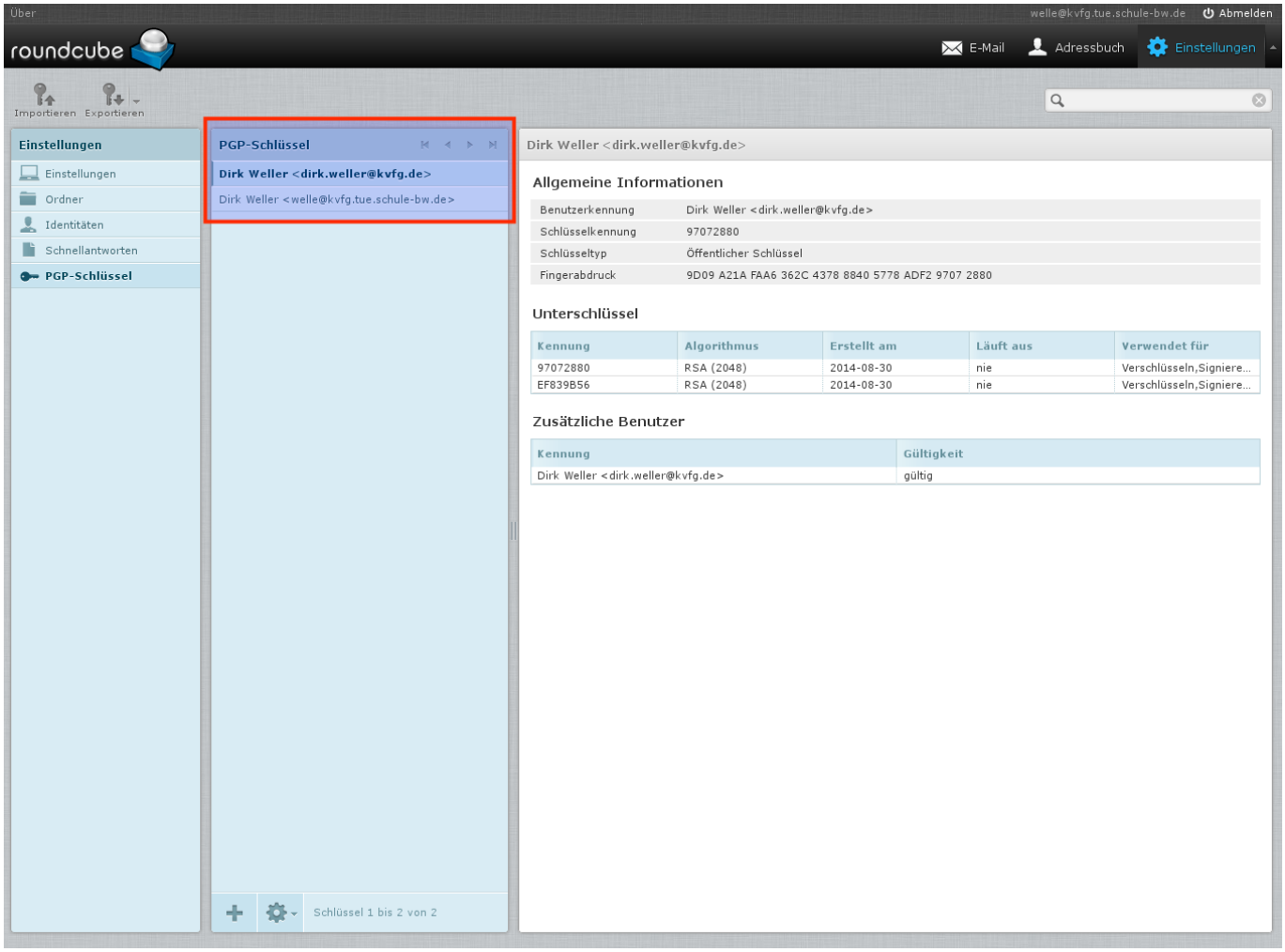


Jetzt kannst Du die Mail im entschlüsselten Klartext lesen.

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!

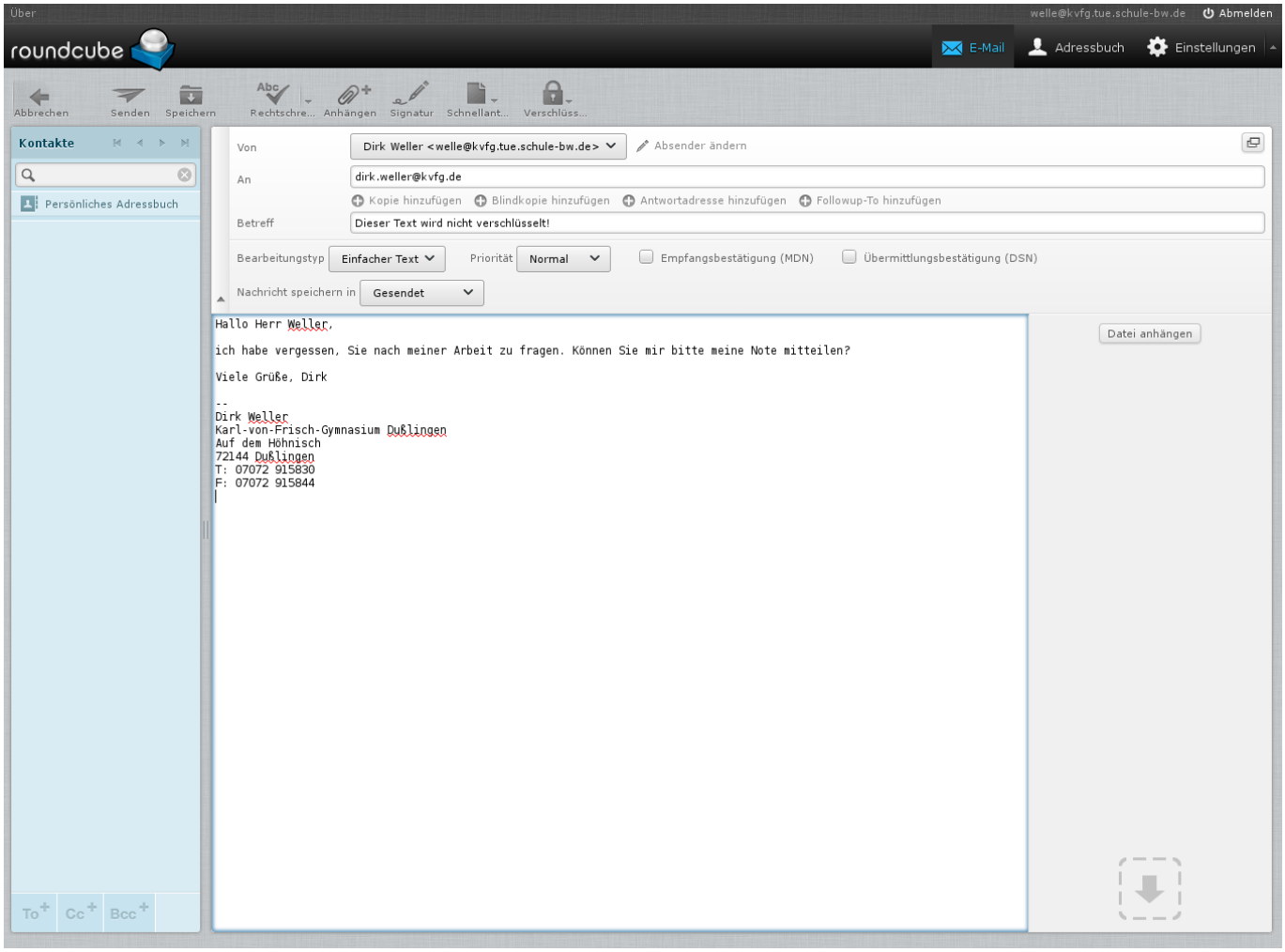


Wenn Du die von Dir bereits eingesammelten Schlüssel ansehen willst, dann klick auf

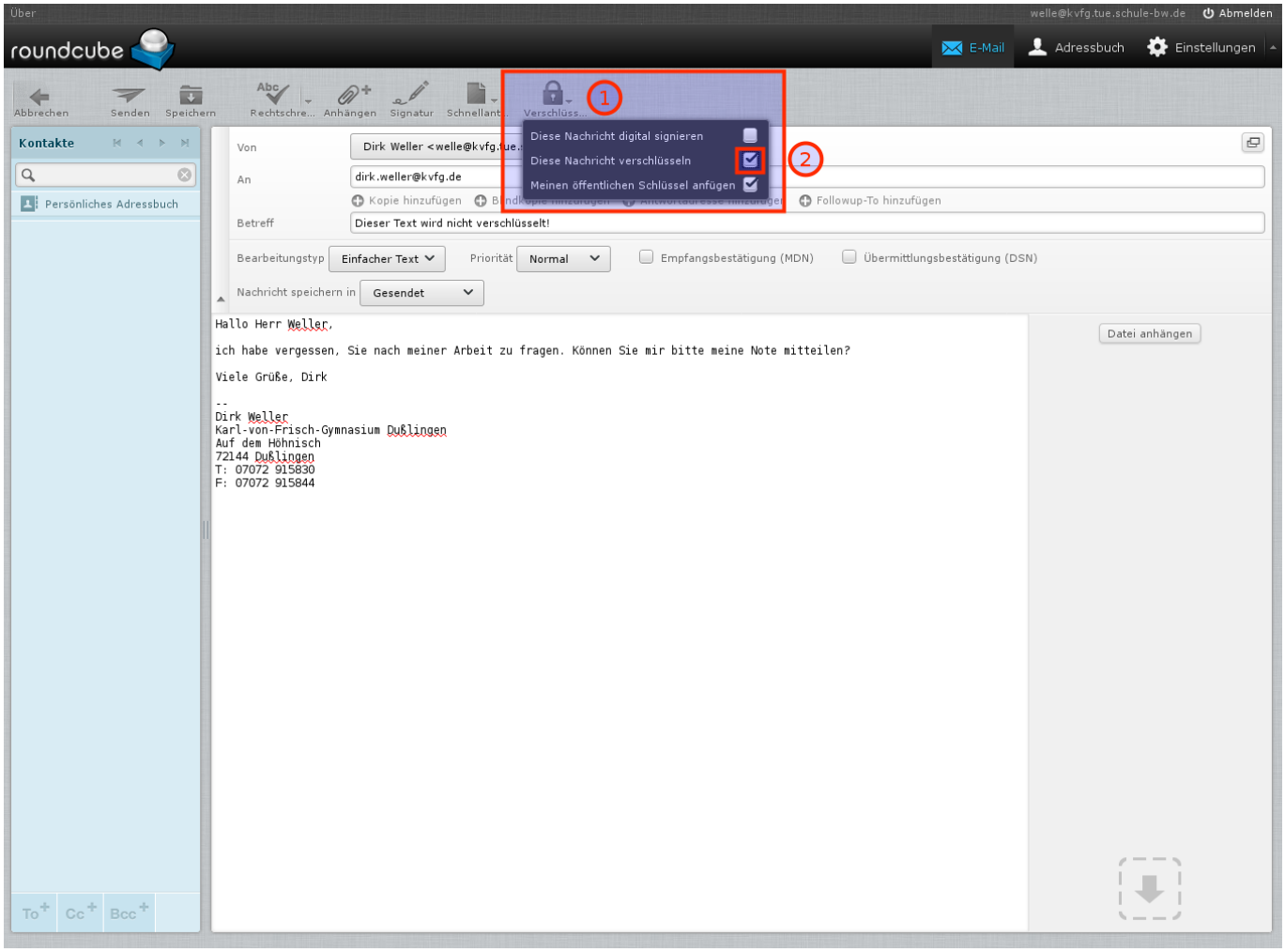
- Einstellungen
- PGP-Schlüssel

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.