

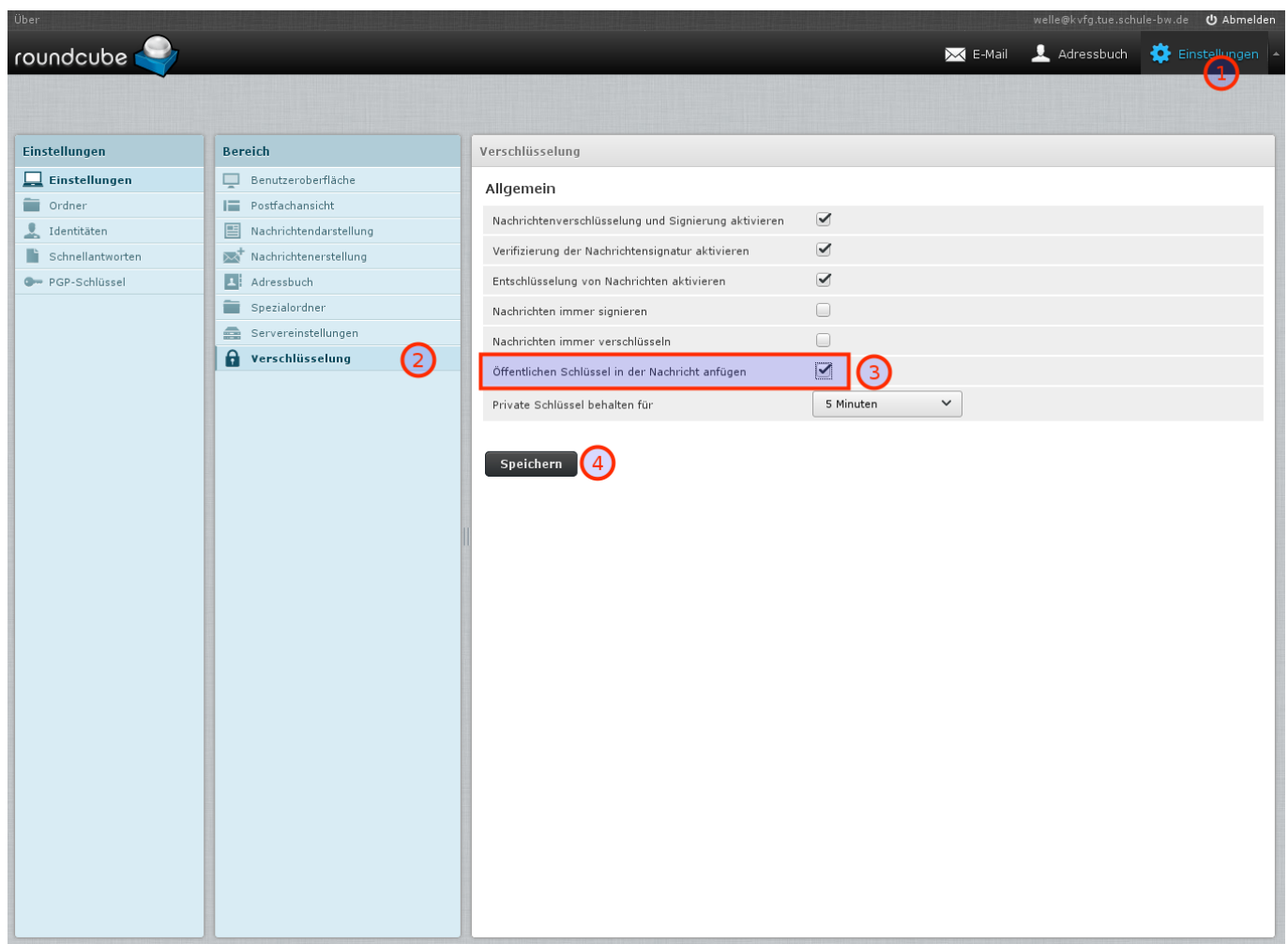
# PGP Verschlüsselung für Schüler/innen

Die folgende Anleitung beschreibt, wie Ihr Euch einen PGP-Schlüssel für Eure 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.

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!

The screenshot shows the Roundcube webmail interface for user Dirk Weller. The left sidebar has a menu with 'Einstellungen', 'Ordner', 'Identitäten', 'Schnellantworten', and 'PGP-Schlüssel'. The main area shows 'PGP-Schlüssel' for Dirk Weller. A dialog box 'Schlüssel exportieren' is open, asking 'Möchten Sie geheime Schlüssel in die gespeicherte OpenPGP-Schlüsseldatei mit aufnehmen?'. It has two buttons: 'Nur öffentliche Schlüssel exportieren' and 'Geheime Schlüssel exportieren', with the latter highlighted by a red rectangle. In the background, there are tables for 'Allgemeine Informationen' and 'Unterschlüssel'.

Benutzerkennung	Dirk Weller <welle@kvfg.tue.schule-bw.de>
Schlüsselkennung	21BE497F
Schlüsseltyp	Schlüsselpaar
Fingerabdruck	6DDF 0EB3 DF43 5B2E 4F37 9DF8 8B80 B3E0 21BE 497F

Kenntnis	Algorithmus	Erstellt am	Läuft aus	Verwendet für
		17-04-18	nie	Signieren, Bestätigen
		17-04-18	nie	Verschlüsseln

Gültigkeit
gültig

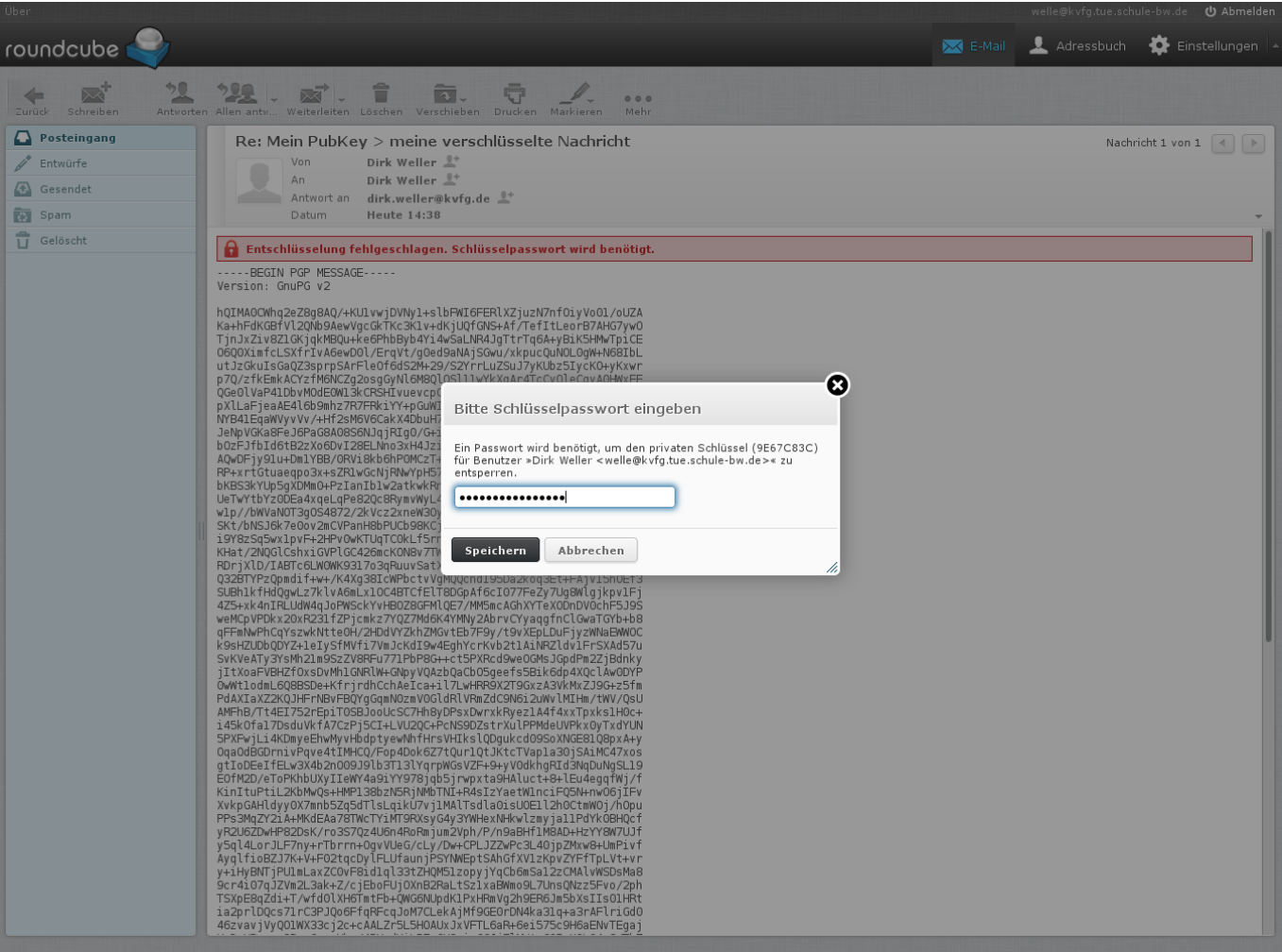
Dein Schlüsselbund liegt nun auf unserem Server und ist nur durch das Passwort geschützt, das Du diesem gegeben hast. Zur Sicherheit (z.B. falls der Server mal über die Wupper geht) solltest Du Dir Deinen Schlüsselbund herunterladen. Dazu klickst Du

- 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

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

Permanent link:  
<https://www.kvfg.net/wiki/doku.php?id=netz:pgp4sus&rev=1492520892>

Last update: 2017/04/18 15:08

