

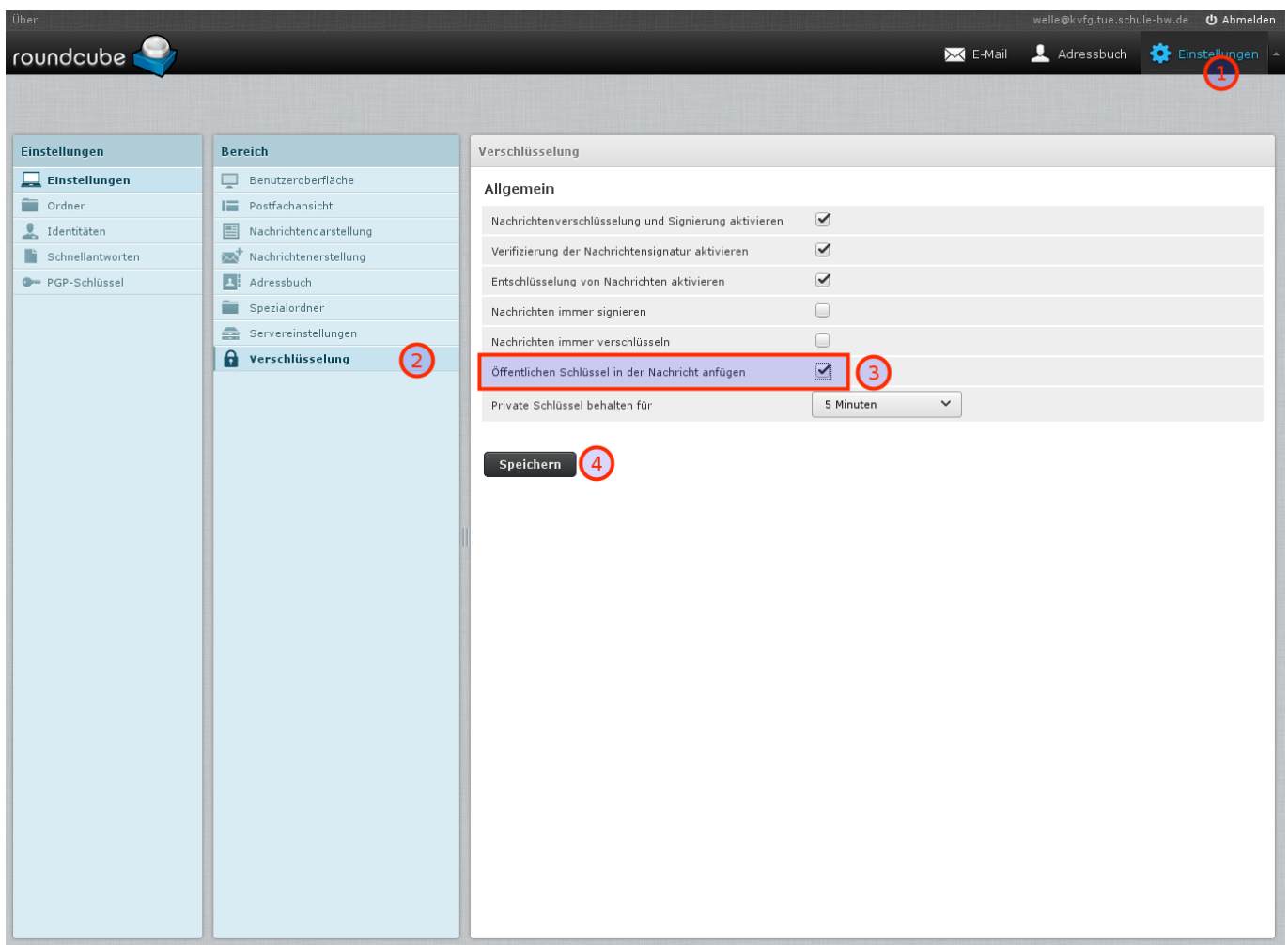
PGP Verschlüsselung für Schüler/innen

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.

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!

The screenshot shows the Roundcube webmail interface for user Dirk Weller. The left sidebar has 'PGP-Schlüssel' selected. The main area shows 'Allgemeine Informationen' and 'Unterschlüssel'. 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.

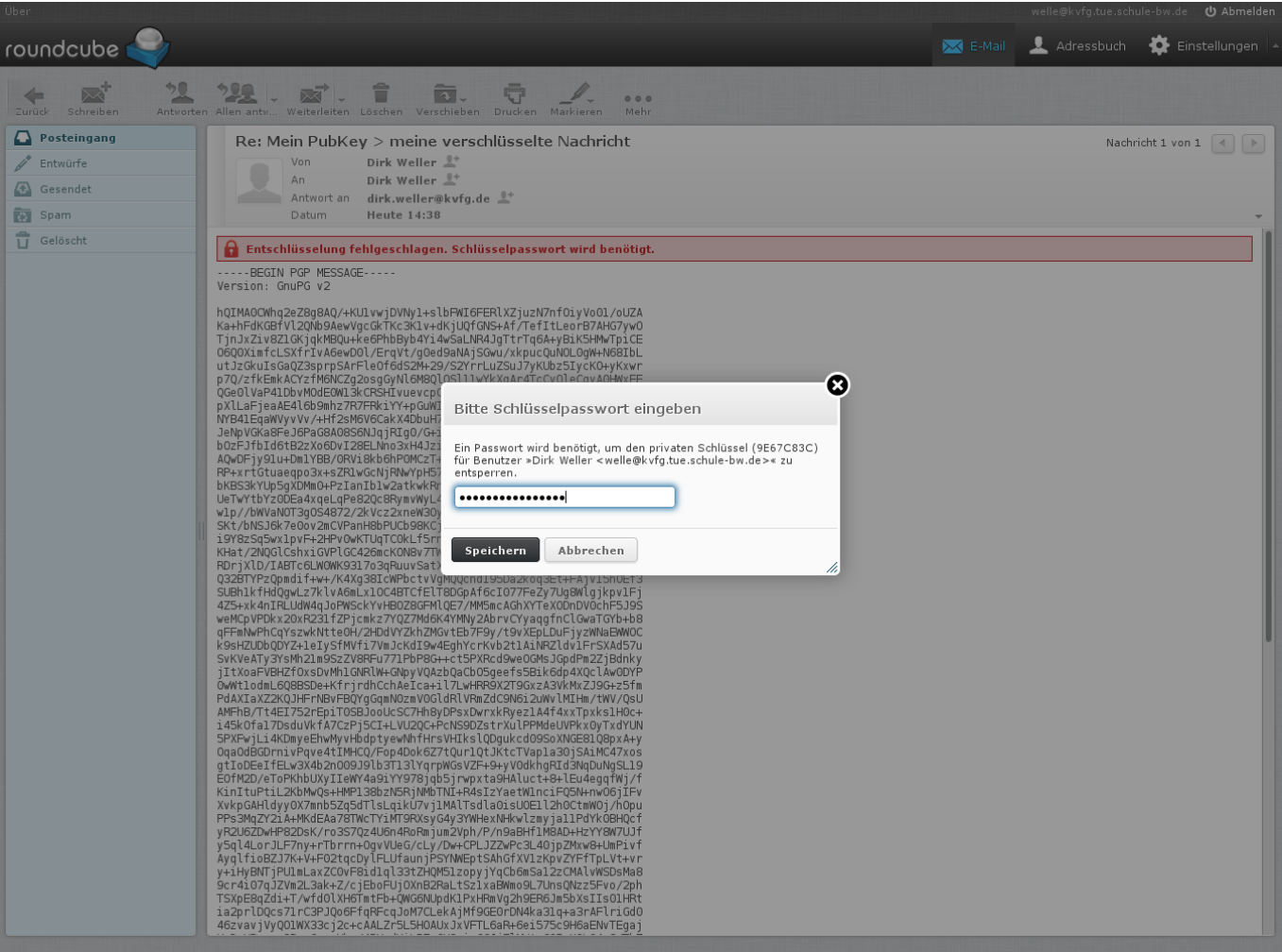
Dein Schlüsselbund liegt nun auf unserem Server, ist aber nur durch das Passwort geschützt, das Du diesem gegeben hast. Zur Sicherheit (z.B. falls der Server mal über die Wupper geht) solltest Du Dir Deinen Schlüsselbund herunterladen. Dazu klickst Du

- auf Exportieren
- Geheime Schlüssel exportieren

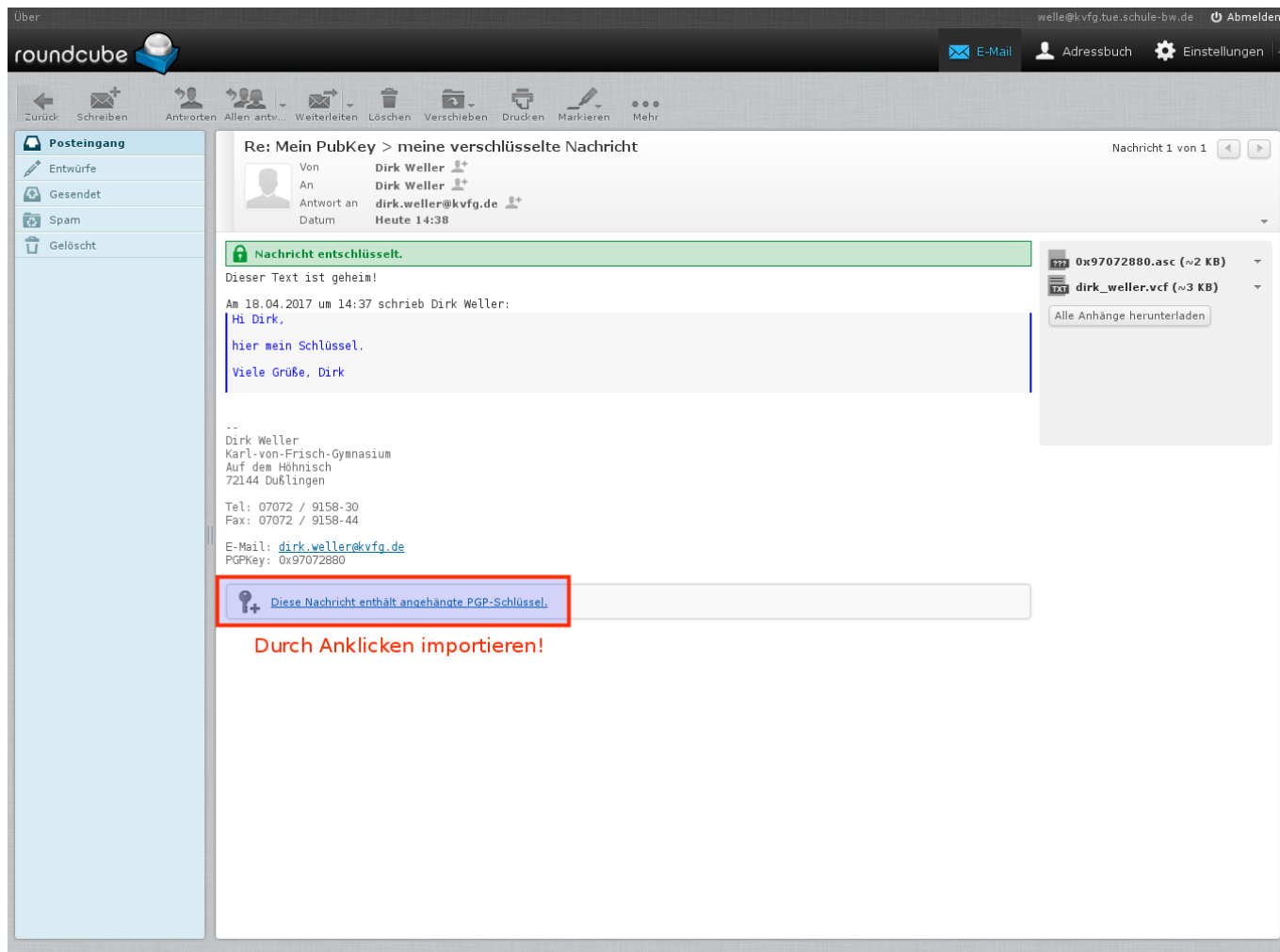
und speicherst die Datei lokal so weg, dass außer Dir keiner da dran kommt. Ein VeraCrypt-Container ist eine gute Wahl!

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 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. The left sidebar has a menu with 'Einstellungen' and 'PGP-Schlüssel' highlighted. The main area displays the PGP key management section for 'Dirk Weller <dirk.weller@kvfg.de>'. The 'PGP-Schlüssel' tab is selected, showing a list of keys. The 'Allgemeine Informationen' section displays the user's name, email, and key ID. The 'Unterschlüssel' section shows a table of subkeys. The 'Zusätzliche Benutzer' section shows a table of additional users.

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...

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

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

roundcube E-Mail Adressbuch Einstellungen

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

Kontakte

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

An dirk.weller@kvfg.de

Betreff Dieser Text wird nicht verschlüsselt!

Kopie hinzufügen Blindkopie hinzufügen Antwortadresse hinzufügen Followup-To hinzufügen

Bearbeitungstyp Einfacher Text Priorität Normal

Empfangsbestätigung (MDN) Übermittlungsbestätigung (DSN)

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

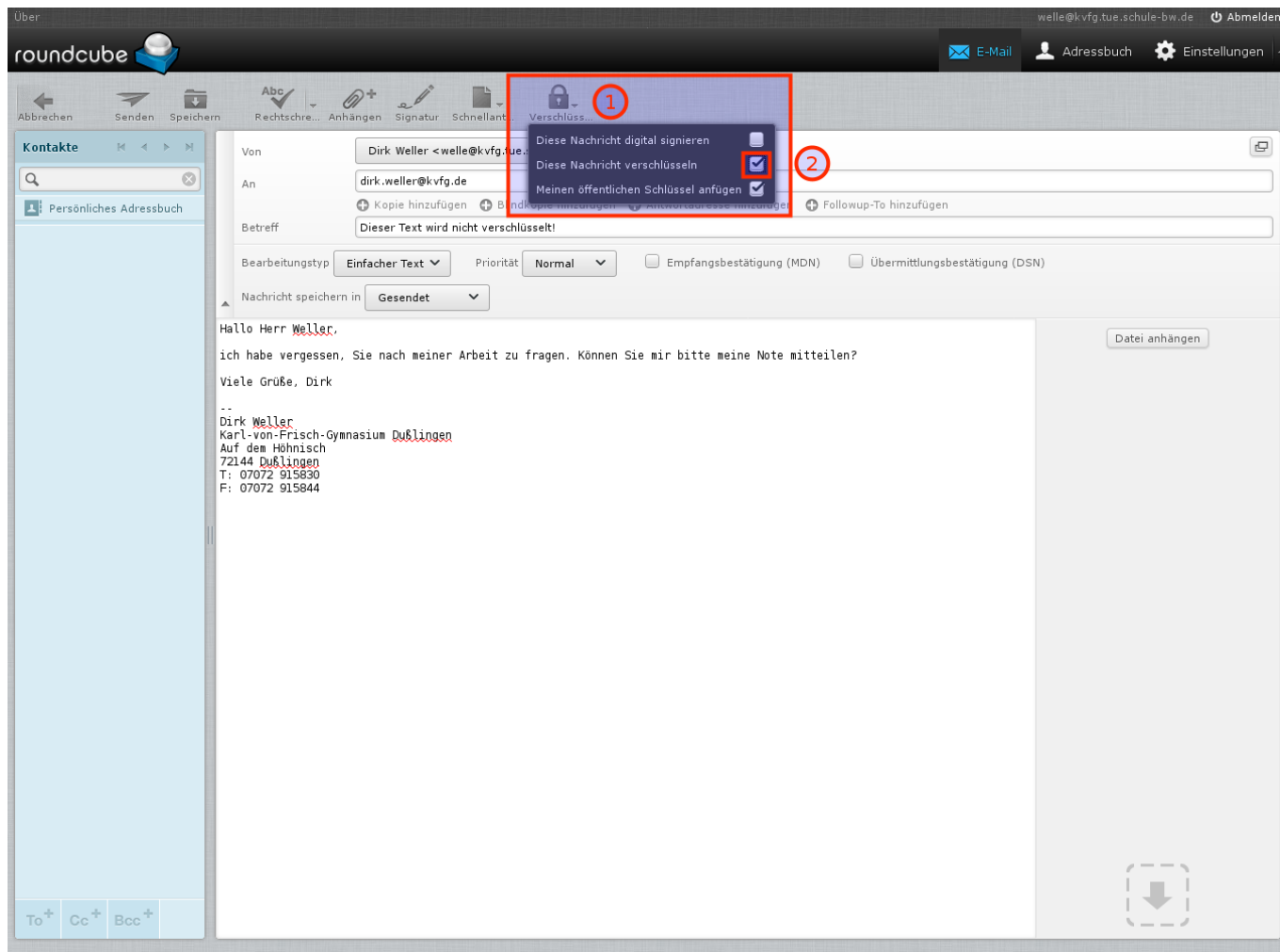
--

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=1492523945>

Last update: **2017/04/18 15:59**

