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-schule.de an:

https://webmail.kvfg-schule.de

Über						ile-bw.de 🙂 Abmelden
roundcube 🍣				🔇 E-Mail	👤 Adressbuch	🔅 Einstellungen 🔺
						(1)
Einstellungen	Bereich	Verschlüsselung				
🛄 Einstellungen	💻 Benutzeroberfläche	Allgemein				
Crdner Ordner	Postfachansicht	Nachrichtenverschlüsselung und Signierung aktivieren				
L Identitäten	Nachrichtendarstellung					
Schnellantworten	Nachrichtenerstellung	verifizierung der Nachrichtensignatur aktivieren				
PGP-Schlüssel	Adressbuch	Entschlüsselung von Nachrichten aktivieren				
	Spezialordner	Nachrichten immer signieren				
	A verschlüsselung	Nachrichten immer verschlüsseln				
	verschlusselung	Öffentlichen Schlüssel in der Nachricht anfügen				
		Private Schlüssel behalten für	5 Minuten 🗸			
		Speichern 4				

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.

Uber					welle@kvfg.tue.sch	ule-bw.de 🕐 Abmelden
roundcube				E-Mail	Adressbuch	Einstellungen
Importieren Exportieren					٩	8
Einstellungen	PGP-Schlüssel 🛛 🕅 🔺 🕨	Neues Schlüsselpaar e	erstellen			
Einstellungen Ordner Identitäten Schnellantworten PGP-Schlüssel		Identität: Schlüssellänge: Passwort: Passwort bestätigen: Speichern 4	Dirk Weller <welle@kvfg.tue.schule-bw.de> ¥</welle@kvfg.tue.schule-bw.de>	3		
1	+ Chiussel gefunden					

Im nächsten Schritt erzeugst Du Dein Schlüsselpaar für benutzer@kvfg-schule.de (im Bild oben steht noch die alte Maildomain). "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!

Über						welle@kvfg.tue.scl	nule-bw.de 🛈 Abmelden
roundcube 🍣					🔀 E-Mail	💄 Adressbuch	🔅 Einstellungen 🔺
Importieren Exp						٩	
Einstellungen	PGP-Schlüssel ⋈ ∢ ≻ ⋈	Dirk Weller <welle@k< td=""><td>vfg.tue.schule-bw.de></td><td></td><td></td><td></td><td></td></welle@k<>	vfg.tue.schule-bw.de>				
Einstellungen	Dirk Weller <welle@kvfg.tue.schule-bw.de></welle@kvfg.tue.schule-bw.de>	Allgemeine Inforn	nationen				
Ordner		Benutzerkennung	Dirk Weller < welle@ky	fa tue schule-hw de>			
👤 Identitäten		Schlüsselkennung	21BE497F	ingitaleteenate entitiee			
Schnellantworten		Schlüsseltyp	Schlüsselpaar				
🗫 PGP-Schlüssel		Fingerabdruck	6DDF 0EB3 DF43 5B2	E 4F37 9DF8 8B80 B3E0 :	21BE 497F		
		Unterschlüssel					
		Kennung	Algorithmus	Tellt am	Läuft a	us V	erwendet für
				17-04-18	nie	s	ignieren,Bestätigen
	Schlüss	sel exportieren)17-04-18	nie	V	erschlüsseln
	Möchten S Schlüsseld Geheim	ie geheime Schlüssel in die datei mit aufnehmen?	ieren		,keit		

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 \checkmark - 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.

ዕ Abmelden

Jetzt kannst Du die Mail im entschlüsselten Klartext lesen.

P Diese Nachricht enthält angehängte PGP-Schlüssel. Durch Anklicken importieren!

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!

2024/04/28 22:49	5/8	PGP Verschlüsselung für Schüler/inne				
ber		weile@kvfg.tue.schule-bw.de 😃 Abmeld				
oundcube 🥰		🔀 E-Mail 👤 Adressbuch 🔅 Einstellungen				
Zurück Schreiben A	12. 128 - 1 1 1 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1					
Posteingang	Re: Mein PubKey > meine verschlüsselte Nachricht	Nachricht 1 von 1 🔳 🕨				
Gesendet	An Dirk Weller 1*					
Spam	Antwort an dirk.weller@kvfg.de 14:38					
Gelöscht	Rachricht entschlüsselt.	- 0-070707080 (-2 KB)				
	Dieser Text ist geheim!	UR97072000.dst (~2 KB) *				
	Am 18.04.2017 um 14:37 schrieb Dirk Weller:					
	Hi Dirk,	Alle Annange herunterladen				
	hier mein Schlüssel.					
	Viele Grüße, Dirk					
	Dirk Weller					
	Karl-von-Frisch-Gymnasium Auf dem Höhnisch					
	72144 Dußlingen					
	Tel: 07072 / 9158-30 Fax: 07072 / 9158-44					
	E-Mail: <u>dirk.weller@kvfg.de</u>					
	PGPKey: 0x97072880					

roundcube 🍣					🔇 E-Mail	L Adressbuch	Einstellungen
Importieren Exportieren						Q	8
Einstellungen	PGP-Schlüssel K ∢ ► N	Dirk Weller < dirk.wel	ler@kvfg.de>				
Einstellungen Ordner Identitäten Schnellantworten PGP-Schlüssel	Dirk Weller <dirk.weller@kvfg.de> Dirk Weller <welle@kvfg.tue.schule-bw.de></welle@kvfg.tue.schule-bw.de></dirk.weller@kvfg.de>	Allgemeine Inform Benutzerkennung Schlüsselkennung Schlüsseltyp Fingerabdruck	Allgemeine Informationen Benutzerkennung Dirk Weller < dirk.weller@kvfg.de> Schlüsselkennung 97072880 Schlüsseltyp Öffentlicher Schlüssel Fingerabdruck 9D09 A21A FAA6 362C 4378 8840 5778 ADF.				
		Unterschlüssel Kennung 97072880 EF839B56 Zusätzliche Benut	Algorithmus RSA (2048) RSA (2048) Zer	Erstellt am 2014-08-30 2014-08-30	Läuft au nie nie	15	Verwendet für Verschlüsseln,Signiere Verschlüsseln,Signiere
		Zusätzliche Benut Kennung Dirk Weller < dirk.welle	zer r@kvfg.de>	Gültigke gültig	it		
	+ 🔅 - 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



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!

7/8



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=1503207493



Last update: 2017/08/20 07:38