## Mailverschlüsselung

Voraussetzungen:

- E-Mail-Client (z. B. Thunderbird)
  - o AddOn: Enigmail
- Gpg4win

Vorgehensweise:

- Installation des Mailclients (soweit dies noch nicht geschehen ist)
- Installation des AddOns Enigmail (Extras -> Addons -> suchen nach Enigmail -> Installieren und Thunderbird neu starten -> fertig)



- Installation Gpg4win wie folgt (sollten Fenster auftauchen, die hier nicht gesondert aufgelistet sind, so wird in diesen nichts weiter verlangt, als auf "weiter" zu klicken):

December

## Download Gpg4win:

			Dowmoad
Google	gpg4win	I Q	Free Software for free download.
	Web         Images         Maps         Sbopping         Videos         More -         Search tools           About 177 0000 results (0.200 seconds)         Coaties help us deliver our services. By using our services, you agree to our use of coaties.         Coaties help us deliver our services.         Search tools		Gpg4win 2.2.0-beta (Released: 2013-07-16) Current beta version of Opp4win 2.2.0 with improvements in OppEx, Opp0L, OnuPG, Pinentry and Kalopatra, in different variants available • End investing: 30 Motuci () QueGPCP singestow
	$\begin{array}{llllllllllllllllllllllllllllllllllll$		Upht Installer (13 MByte, vethout Kloopatra and Gpg4vin Compandium)   OpanPGP signatur Vanilla installer (4 MByte, Gru/PG only)   OpanPGP signature Oueflext installer (319 MByte)   OpanPGP signature README All Beta versionen and OpanPGP signatures: files.gpg4vin.org/Beta/.
	Download Gogdwin         Eastures           You can dowload the full version (including the Gogdwin         Features. The security of your data the most important thing. The           More results from gpgdwin org >	is	
	Gpg4win - Sichere E-Mail- und Datei-Verschlusselung mit GnuPG     www.gpg4win.de/ ~ Translate this page     Gpg4win 2.2.0-beta2 veröfentlicht Gpg4win 2.1.1-beta197 veröfentlicht Gpg4w     GRU Phace Veröfentlicht Gpg4win 2.1.1-beta197 veröfentlicht Gpg4w     GRU Phace Veröfentlicht Gpg4win 2.1.1-beta197 veröfentlicht	win	Gpg4win 2.1.1 (Released: 2013-05-31) You can download the full version (including the Gpg6win compendium) of Gpg6win 2.1.1 here:
	Construin - Whitnesdia, the free encyclopedia on wispedia organistic <b>Departmin</b> + <b>Copyloni</b> is an installation package for Windows (29, Vista and 7) with asthware tools and manuals for email and file encryption on behalf of the German	0	Gpg4Win 2.1.1 Eter 35 Mb/W OpenPGP signature (for gpg4win2.1.1.ev) SHAI checksum (for gpg4win2.1.1.ev) SHAI checksum (for gpg4win2.1.1.ev)
	Gpg4win — Wikipedia de wikipedia ong/wiki/Opg4win * Translate this page Gpg4win (RUX) Prokey Guad for Windows) ist ein Installationspaket für Windows (VP/Vista#) mit Cemputer-Programmen und Handbüchem zur E-Mail- und		Changelog More Gpg4win-2.1.1 variants

Installation: bitte die Installation einfach durchklicken und die Fragen mit OK bestätigen bis das zweite Fenster zu sehen ist (Fertig):



Jetzt auf "Weiter" klicken: hier bitte das Häkchen unten in das entsprechende Feld machen.

	<u> _</u>
Gro D	Vertrauenswürdige Wurzelzertifikate festlegen S/MIME-Konfiguration
Gpg4win braucht eine Li	iste mit Wurzelzertifikaten, denen Sie vertrauen.
(Um S/MIME-Zertifikate müssen Sie die Vertraue festlegen.)	zum Signieren und Verschlüsseln zu verwenden, enswürdigkeit der X.509-Wurzelzertifikate
Ein Wurzelzertifikat (au untergeordneten Zertif vertraut, so vertraut m Zertifikaten.	uch: Root-CA) dient dazu, die Gültigkeit aller fikate zu überprüfen. Wird dem Wurzelzertifikat nan damit auch allen darunter liegenden
) Damit Sie S(MIME nutze) Sie diese som sie Sie	n können, ist die Konfiguration zwingend erforderlich. Überspringen kein S/MIME nutzen möchten.
ble diese nur, wenn ble	
Sie diese nur, wenn be ▼ Wurzelzertifikate fes	stgelegt oder Konfiguration überspringen
Wurzelzertifikate fes ₩ Wurzelzertifikate fes	stgelegt oder Konfiguration überspringen 16-7

Im nächsten Schritt wird die Konfiguration abgeschlossen und Ihr könnt die Readme-Datei lesen (oder auch nicht).

Nachdem das Add-on installiert wurde, taucht nach dem Neustart im Thunderbird-Menü das Feld "OpenPGP" auf.



Als nächstes müssen die Schlüssel angelegt werden. Es werden zwei Schlüssel erstellt: Der öffentliche Schlüssel zum Verschlüsseln von Mails. Diesen Schlüssel müsst Ihr später an den Mailempfänger weitergeben mit dem Ihr verschlüsselt kommunizieren wollt. Der private Schlüssel wird zur Entschlüsselung von E-Mails benötigt. Diesen Schlüssel müsst Ihr gut abspeichern (CD oder USB-Stick; am besten zweimal sichern).

Klickt bitte auf "OpenPGP" und geht auf "Schlüssel verwalten". Hier klickt bitte auf "Erzeugen" und dort auf "neues Schlüsselpaar":

Das nächste Fenster ist sehr wichtig. Hier wird unter "Passphrase" ein Passwort verlangt, das Komplex, aber dennoch merkbar sein sollte. Nehmt also eines, das mindestens 8 Zeichen lang ist, Großbuchstaben und Sonderzeichen, sowie Zahlen enthält (z. B. 1.FC\_Schalke04!)

🔄 OpenPGP-Schlüssel erzeugen 📃 🗌 🗙						
Benutzer-ID Richard Fülle <richard.fuelle@lai.de> - richard.fuelle@lai.de</richard.fuelle@lai.de>						
Schlüssel zum Unterschreiben verwenden						
keine Passphrase						
Passpirase ••••••••• Passphrase (wiederholen)						
Kommentar Fußball						
Ablaufdatum Erweitert						
Schlüssel läuft ab in 5 Jahren 🔻 🔽 Schlüssel läuft nie ab						
OpenPGP-Bestätigung						
Erzeuge öffentlichen und privaten Schlüssel für "Richard Fülle (Fußball) <richard.fuelle@lai.de>"</richard.fuelle@lai.de>						
Schlüsselpaa Schlüssel erzeugen Abbrechen						
Konsole zum Erzeugen eines Schlüssels						
ALHTUNG: Das Erzeugen eines Schlussels kann mehrere Minuten dauern, beenden bie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.						

Nachdem die Schlüssel angelegt wurden, wird dazu aufgefordert, ein Widerrufszertifikat zu erzeugen. Bitte macht das auch und speichert es dort ab, wo Ihr es wieder finden könnt:

OpenPGP	P-Bestätigung			
?	Erzeugen des Schlüssels abgeschlossen. Benutzer-ID <richard.fuelle@lai.de> wird zum Unterschreiben verwendet.</richard.fuelle@lai.de>			
	Es wird dringend empfohlen, dass Sie nun ein Widerrufszertifikat für Ihren Schlüssel erzeugen. Dieses Zertifikat benötigen Sie, um Ihren Schlüssel bei Bedarf für ungültig zu erklären (z.B. wenn der Schlüssel missbraucht, verloren oder gestohlen wird).			
	Möchten Sie nun das zugehörige Widerrufszertifikat erzeugen?			
	Zertifikat erzeugen Abbrechen			

Grundsätzlich funktioniert nun die Verschlüsselung. Solltet Ihr mit jemandem verschlüsselte Mails austauschen wollen, müsst Ihr dem jeweiligen Partner/in Euren öffentlichen Schlüssel zukommen lassen:

Öffnet hierzu eine neue E-Mail, klickt auf OpenPGP und wählt "Meinen öffentlichen Schlüssel anhängen":

	Busicie Zeitonen	OpegPGP Egtras Hilfe	
Senden 👘	isanar - 🥥 Ar	Nachricht unterschreiben Strg+Umschalt+S Nachricht verschlüsseln Strg+Umschalt+E	perhern +
yon	Rich and Fulle <nich< td=""><td>EGP/MIME verwenden</td><td></td></nich<>	EGP/MIME verwenden	
An	8	Schlüssel verwaken Verschlüsselung rückgängig machen Meinen öffentlichen Schlüssel anhängen	
		Hife	
Betzeff			

Solltet Ihr ab jetzt E-Mails verschlüsselt senden, kommen diese beim Empfänger so an, wenn sie dieser nicht entschlüsselt oder entschlüsseln kann:

Von: Juergen Lehle <u>(uergen.lehle@lai.de&gt;</u> Datum: 20.07.2013 13:20 (GMT+01:00) An: Simone und Richard Fülle <u>⊲ichard.tuelle@lai.de&gt;</u> Betreff: Re: Verschlüsselung BEGIN PGP MESSAGE Charset: UTF-8 Version: GnuPG v2.0.21-beta20 (MingW32)	Von: Juergen Lehle <juergen.lehle@lai.de> &amp; Betreff: Re: Verschlüsselung Datum: 20. Juli 2013 13:20:20 MESZ An: Simone und Richard Fülle <richard.fuelle@lai.de> Sicherheit:</richard.fuelle@lai.de></juergen.lehle@lai.de>	Anhang
hQIMA9fjesVsZR0mAQ/aVimIBdWGvSmT9N8lhhvnAVSDKcNetvcOicTF2zhz2uy HBvO8HevP3DEqb03XXQIGJ5bMBOFYEkmU32XXDQNmaQMDrJJZU6KK34wQQR TzzPOSRIP82SGLA685zbg4abUaK-mM5V1FyzQTpy7JTVioKmLgWLVnBAUn7Y HIVT1VdsIrsynGzc2DU2FHymQvC3BVbChoC2gktlMhohdmH7UzgnBK47bxONb FOcO2dFg0tkDuGMv87i95JRyXZPGAXPLWGZPSZPYXJmhzJwLEUh3YmGRIsOf YChIVDTwKOBru1FPLAKVOloiLt8al806H8gVq2SxF1g0SZAMukanJl6J450 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y7q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y9q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH+wEY1WNkjCTb04Y9q3 9U10CKA44W1+7eHJAbnIACuLMi05KF8Bedw2/GWDDH2W3KP31H53K5KD0PWDg545 1C4VX10q0K53yCu95xRQ1dexkyrQmo30KD9FNR31ga4YxHa5pf02FMdhu1P 8K82RWq1C6A5He8B4KL9UADA000q7Q/WCR6QN+V8BEUDPWDg545 1C4VX10q0K53yCu95xRQ1dexkyrQmo30KD9FNR31BSN1F8K2DQPWDg545 1C4VX10q0K53yCu95xRQ1dexkyrQmo30KD9FNR31H53K5KD0PWD11P 8K82RWq10C6A5H8B4K41Gh1DDn65H1U4BR301HCq000q7W7WNK5KXH44M0HFEV3862p 1V5XF91KaQ4W4AGh1bDn64B6H14QH535HBQC1MrR0u084mB18dDmrA1p1H7n322 705KF91KaQ4W4AGh1bDn64B6H14DH535HBQC7W1F1BTQ3MAVAH0H2VT35YU4W8276N 102K02L0105189m17C074X4QKh1hvO7W1F1BTQ3MQCaxkW1qK9FW3 8ARV10CX86B5B0u56G5L9665BV466G749X44Kh1hV01WF1BTQ3KAH0H2VT35YU4W86B5N 102KVK5UMF1HV685M80eEm2XF78WZ28E5BR953Q7X1QmP4mT1NxwK6B8WN 102LVK5UbhaFa4FLdM8H6F70F0DUSPTLyEJmLUqh0584G7TN19MVNGqC073drfr 17UNX072J2L0no1518m1M3W0KPW32L4qK17qQUX6FR82AFH8187gmAACV9K0E 8MbM24p01KVm2LF80b821K24qK17qQUX6FR82AFH8187gmAACV9K0E 8MbM24p04K43UNV6QLB6121+20C4VVW44A0KKR32B5TE913L3U40gH61 4V04BR665B0466G70CV8FFx44V482K448K4X44K80A783H44 9704W84864401LV864X45W3Y3q3BVAU496764D674X1K4864	Nochmal ein Test. Verschlüsselt und mit meinem öffentlichen Schlüssel. Gruß Jürgen Am 20.07.2013 13:00, schrieb Simone und Richard Fülle: > Hallo Jürgen, > ich glaube, die erste Mail war nur signiert und nicht verschlüsselt. > Daher hier eine Mail mit Verschlüsselung. > > Eben doch nicht: ich habe Deinen öffentlichen Schlüssel nicht. Ist es > möglich, dass Du mir den noch schicken musst? > Viele Grüße > Richard > > Ma 20.07.2013 12:21, schrieb Juergen Lehle: >> Dann testen wir mal ob das funktioniert. >> Gruß >> Jürgen >> >> Am 20.07.2013 12:06, schrieb Simone und Richard Fülle: >>> Hallo Jürgen,	
OpenPGP Entschlüsselte Nachricht; Korrekte Unterschrift von Richard Fülle	(Fußball) <richard.fuelle@lai.de></richard.fuelle@lai.de>	Details *
Von Simone und Richard Fülle	🥪 Antworten 🛛 😺 Weiterleiten 🛛 👪 Archivieren 👋 Junk	💢 Löschen

 Open row
 Electric voir Richard rolle (robbal) virtuard r