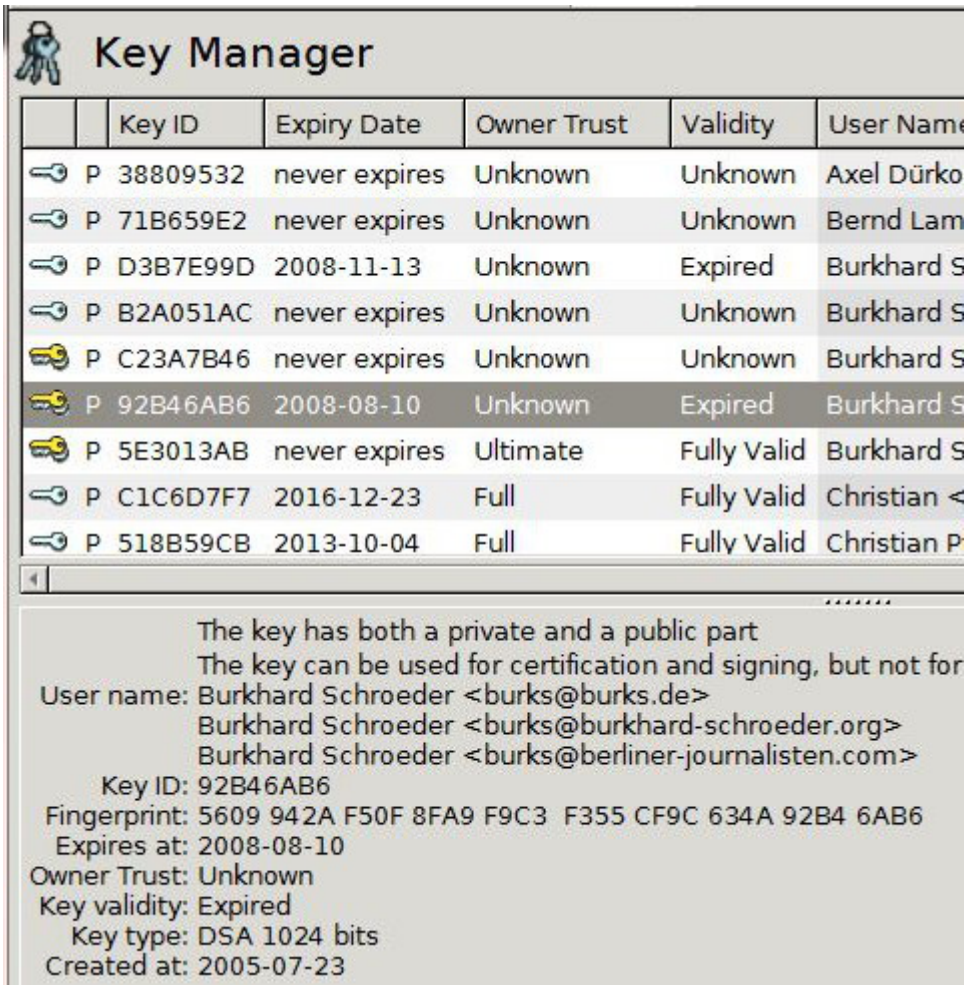
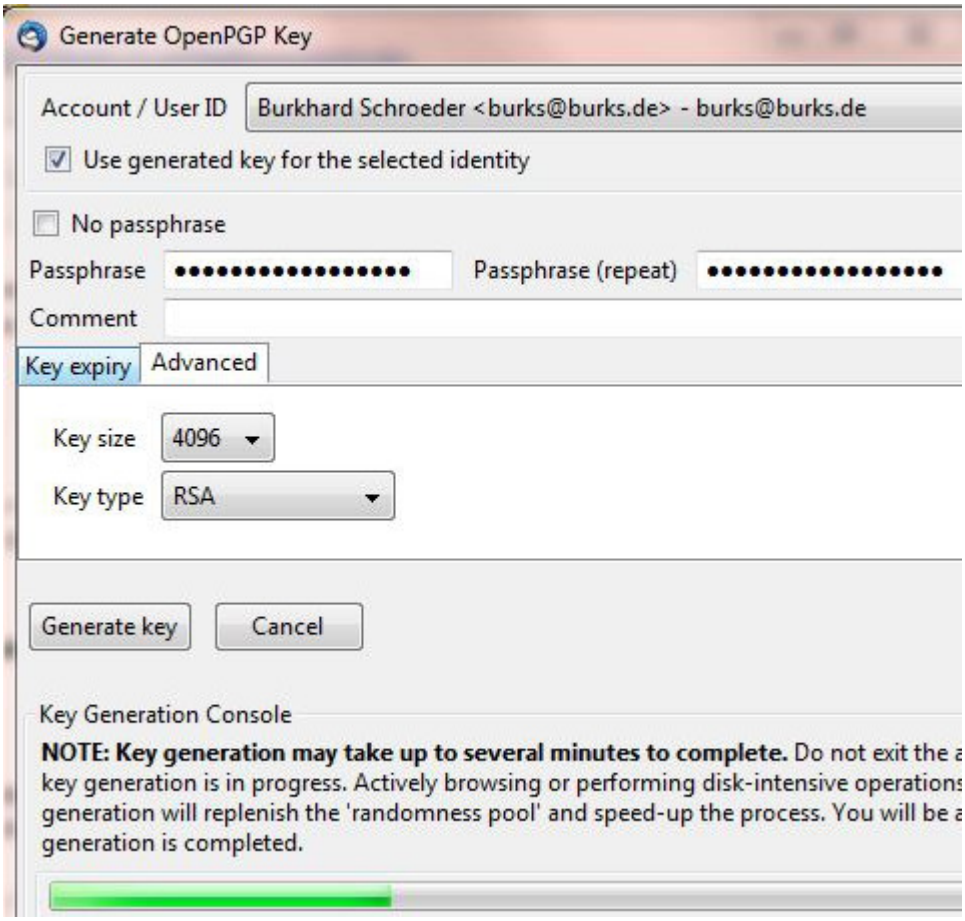
Neuer Schlüssel



Ich habe mit Schrecken gesehen, dass mein Schlüssel schon fast fünf Jahre alt war, ein anderer sogar noch älter (vgl. oben). Zeit, um ihn zu erneuern. Bitte benutzt, um mir eine verschlüsselte E-mail zu schreiben, in Zukunft nur noch diesen:

burks@burks.de(0xC23A7B46)pub.asc – | ID 0x2E47F7D2 | Fingerprint: 6EAA 48C5 C7FB FBCB DA5F 0391 37D5 33B1 2E47 F7D2



Ich musste mich unter Windows wieder ärgern. Nur Enigmail für Thunderbird bietet die Option („advanced“) an, 4096-Bit-Schlüssel zu erzeugen. Kleopatra und der GNU-Privacy-Assistent von GPA btw. Gpg4Win fragen nicht nach oder generieren automatisch schwächere Schlüssel. Wieder ein Argument, dass Programmierer manchmal abschrecken oder verwirren wollen anstatt den Nutzern zu erleichtern, Programme zu benutzen.

Slashdot: „The catch is that the private key needs to be fairly large to be secure: a 4,096-bit RSA key should suffice for some years.“