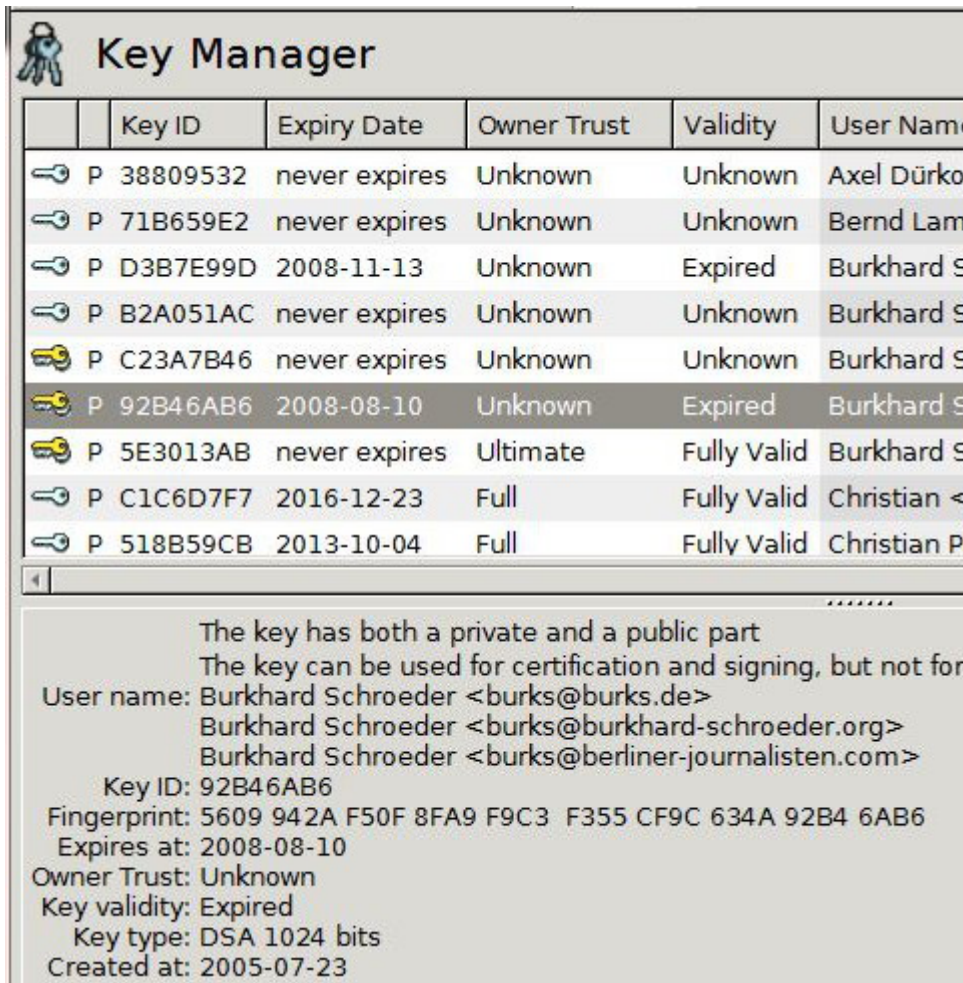


# Neuer Schlüssel



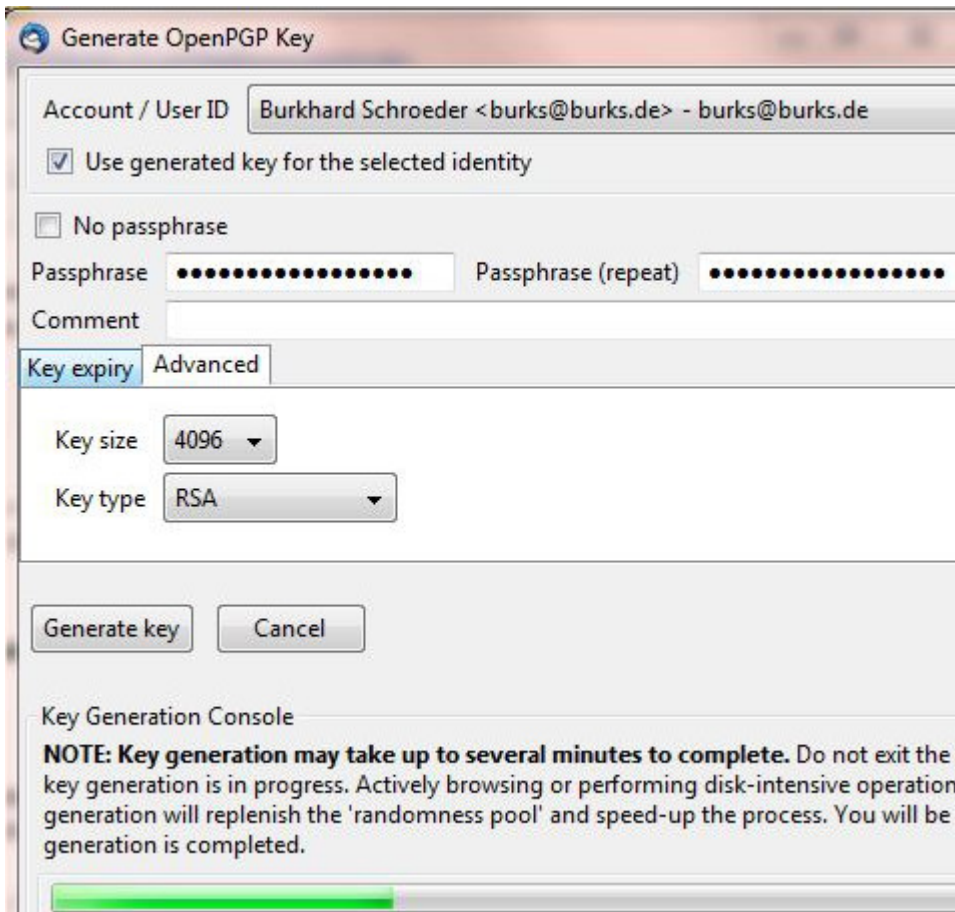
The screenshot shows the 'Key Manager' application window. At the top, there is a title bar with a key icon and the text 'Key Manager'. Below the title bar is a table with the following columns: 'Key ID', 'Expiry Date', 'Owner Trust', 'Validity', and 'User Name'. The table contains several rows of keys. The key with ID '92B46AB6' is highlighted in grey. Below the table, there is a text area displaying details for the selected key:

	Key ID	Expiry Date	Owner Trust	Validity	User Name
← P	38809532	never expires	Unknown	Unknown	Axel Dürko
← P	71B659E2	never expires	Unknown	Unknown	Bernd Lam
← P	D3B7E99D	2008-11-13	Unknown	Expired	Burkhard S
← P	B2A051AC	never expires	Unknown	Unknown	Burkhard S
← P	C23A7B46	never expires	Unknown	Unknown	Burkhard S
← P	92B46AB6	2008-08-10	Unknown	Expired	Burkhard S
← P	5E3013AB	never expires	Ultimate	Fully Valid	Burkhard S
← P	C1C6D7F7	2016-12-23	Full	Fully Valid	Christian <
← P	518B59CB	2013-10-04	Full	Fully Valid	Christian P

The key has both a private and a public part  
The key can be used for certification and signing, but not for  
User name: Burkhard Schroeder <burks@burks.de>  
Burkhard Schroeder <burks@burkhard-schroeder.org>  
Burkhard Schroeder <burks@berliner-journalisten.com>  
Key ID: 92B46AB6  
Fingerprint: 5609 942A F50F 8FA9 F9C3 F355 CF9C 634A 92B4 6AB6  
Expires at: 2008-08-10  
Owner Trust: Unknown  
Key validity: Expired  
Key type: DSA 1024 bits  
Created at: 2005-07-23

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](mailto: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](#) bzw. 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.“