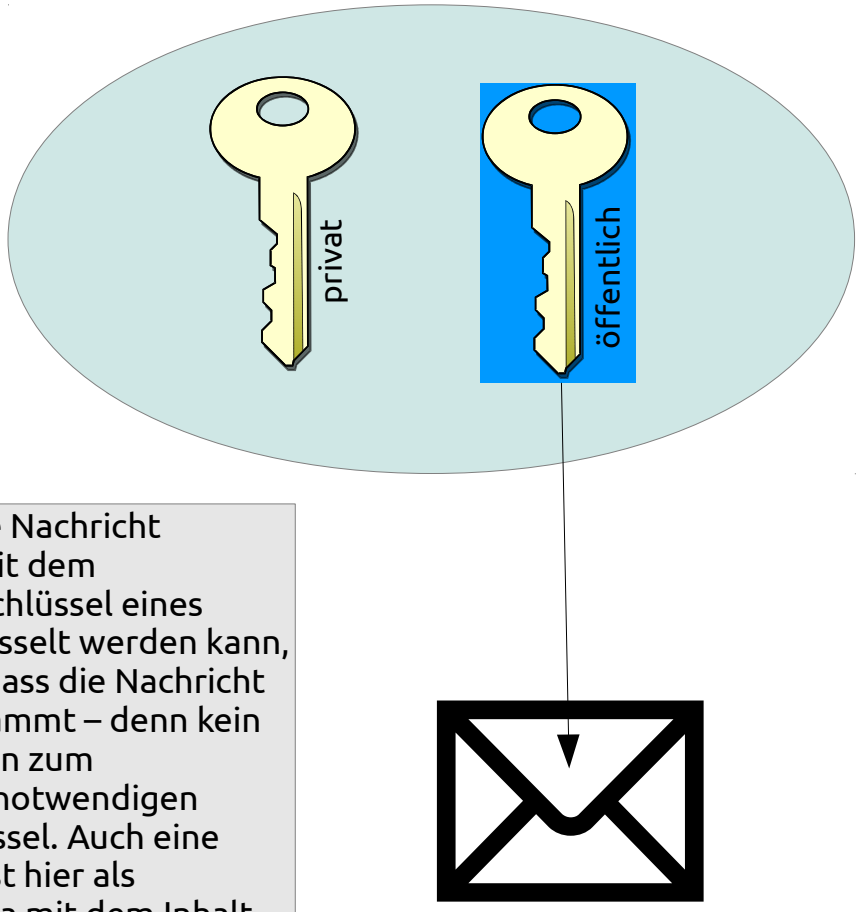
1

Jeder User erzeugt ein *Schlüsselpaar* – einen zum *Verschlüsseln*, und einen zum *Entschlüsseln*. Der erste Schlüssel muss geheim bleiben, während der zum Entschlüsseln öffentlich ist.



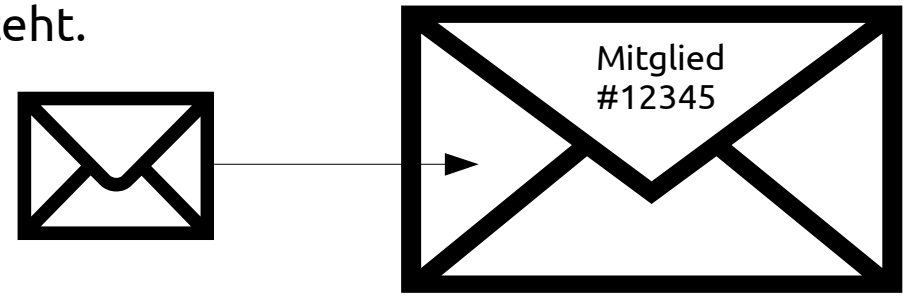
Wenn nun eine Nachricht eintrifft, die mit dem öffentlichen Schlüssel eines Users entschlüsselt werden kann, ist garantiert dass die Nachricht von ihm/ihr stammt – denn kein anderer hat den zum Verschlüsseln notwendigen privaten Schlüssel. Auch eine Abstimmung ist hier als Nachricht (etwa mit dem Inhalt *ja*/*nein*/*Enthaltung*) zu betrachten.

2

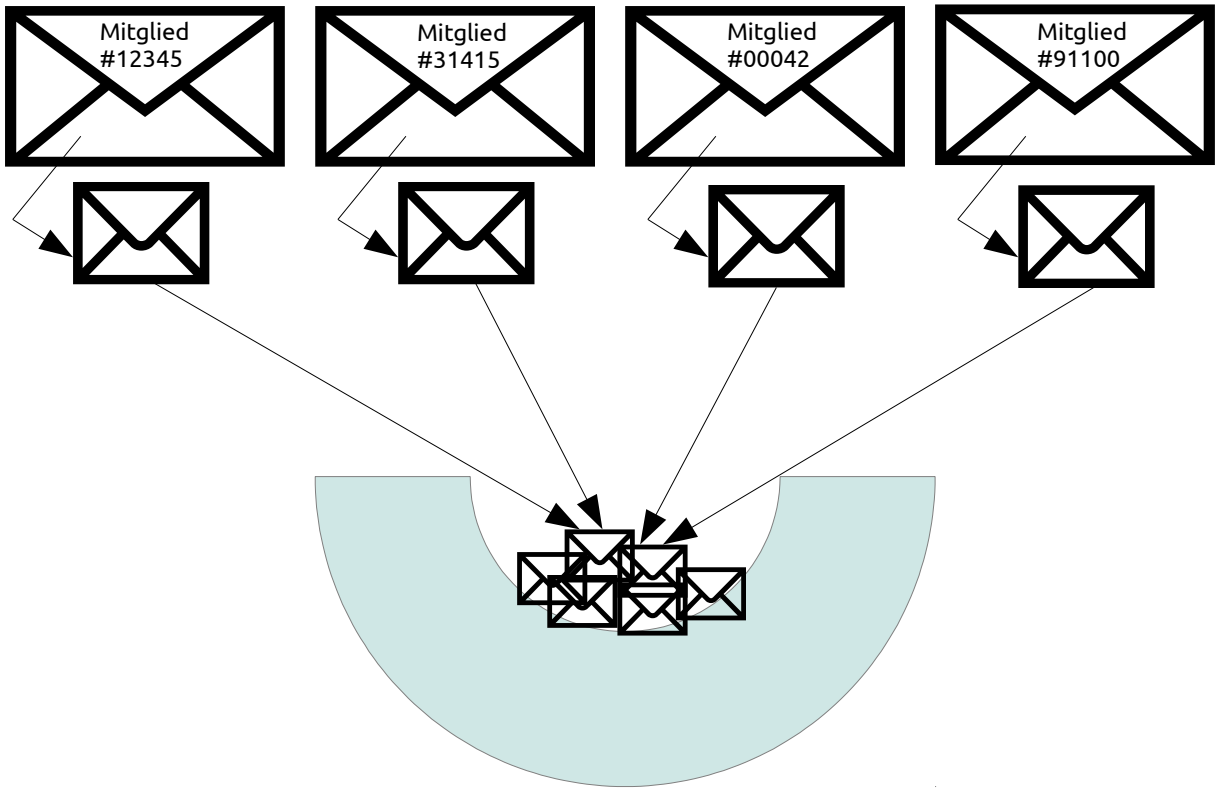
Der öffentliche Schlüssel wird nun in einen neutralen Umschlag getan, damit nicht ersichtlich ist, zu wem dieser Schlüssel gehört.

3

Nun tut jeder den neutralen Umschlag mit seinem öffentlichen Schlüssel in einen weiteren Umschlag, auf dem sein Name steht.



4 Alle Briefe werden gesammelt. Es wird vermerkt, wer einen Brief abgegeben hat. Anschließend werden alle (neutralen) Briefe mit den öffentlichen Schlüsseln in eine Urne getan und vermischt.



5 All diese Schlüssel werden nun in eine Datenbank aufgenommen. Jeder Post im LiquidFeedback, der mit einem dieser Schlüssel entschlüsselt werden kann, stammt also von einem Piraten. Da die Schlüssel aber keiner Person zuordenbar ist, kann jeder weiterhin unter seinem Pseudonym schreiben, ist jedoch trotzdem als „echter“ Pirat authentifiziert.