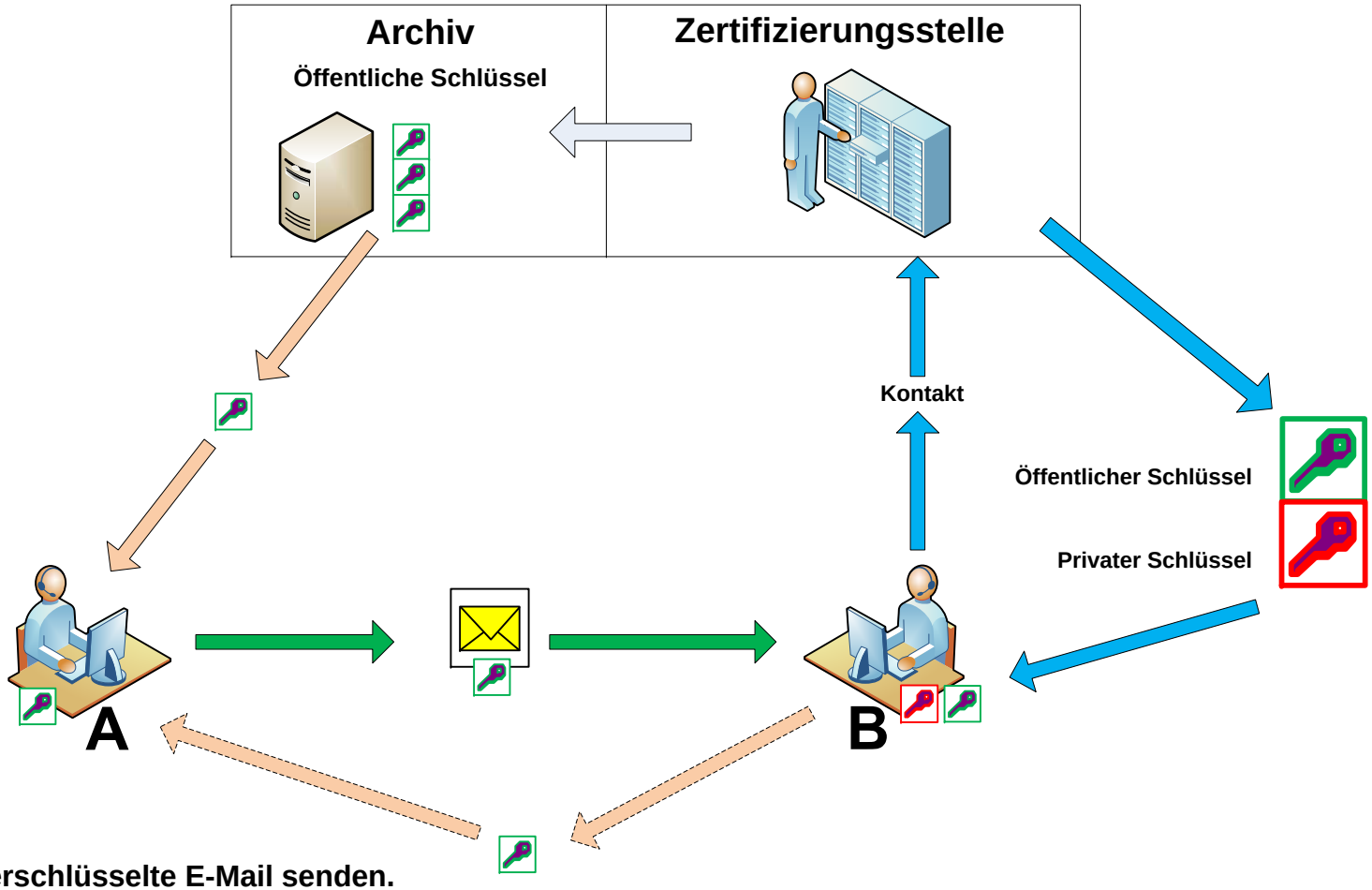

A will an B eine verschlüsselte E-Mail senden.

Zu diesem Zweck muss B ein Schlüsselpaar generieren, bestehend aus einem privaten und einem öffentlichen Schlüssel.
Durch eine Zertifizierungsstelle wird das Schlüsselpaar zertifiziert (Zertifikat erzeugen).

Der geheime, private Schlüssel und auch der öffentliche Schlüssel liegen auf dem Rechner von B.
A verwendet den öffentlichen Schlüssel , um die an B gerichtete E-Mail zu verschlüsseln.
Der Empfänger B kann dann mit seinem privaten Schlüssel die E-Mail wieder entschlüsseln.

Wie kommt A an den öffentlichen Schlüssel von B ?

Entweder (automatisch) aus einer Archivdatei (zertifizierter Server)
oder B schickt A den Schlüssel