# Datenübertragung

## Schritte der Kommunikation

* Übergabe des Briefes mit Link auf App und QR-Code
* Scannen des QR-Codes
* Extraktion des Public Keys aus dem QR-Code und Überprüfung der Signatur
* Ermittlung des Dateinamens aus dem QR-Code
* Herunterladen der Datei
* Entschlüsseln des Session Key, der in der Datei enthalten ist
* Entschlüsseln weiterer Kryptoparameter
* Entschlüsseln des Dokumentes mit den Daten des Trainingsteilnehmers
* Speichern der Daten auf dem Smartphone
* Löschen der Datei auf dem Server

## Arbeitsablauf

* Es gibt einen zentralen Secret Key und dazugehörigen Public Key.
* Für jeden anzulegenden Trainingsteilnehmer wird ein RSA-Key-Pair angelegt. Dieses Keypair dient der Verschlüsselung des Session Keys, mit dem wiederum das eigentliche Dokument verschlüsselt wird.
* Der persönliche Secret Key wird per Brief und QR-Code an den Benutzer geschickt. Im QR-Code befindet sich neben dem Secret Key der Dateiname und die Signatur, die mit dem zentralen Secret Key erstellt wird. Der zentrale Public Key ist in der App enthalten, womit die Signatur und damit die Gültigkeit des persönlichen Secret Key geprüft wird.