SKT-Light und Verschlüsselung sensibler Daten

Betreuer: Prof. Dr. Riedhammer und Franziska Braun

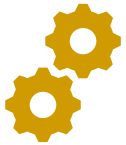
Projektgruppe: Robin Feldmann, Celina Erzen und Celina Bartsch

Präsentation am: 02.06.2022

Gliederung

SKT Test

Demo

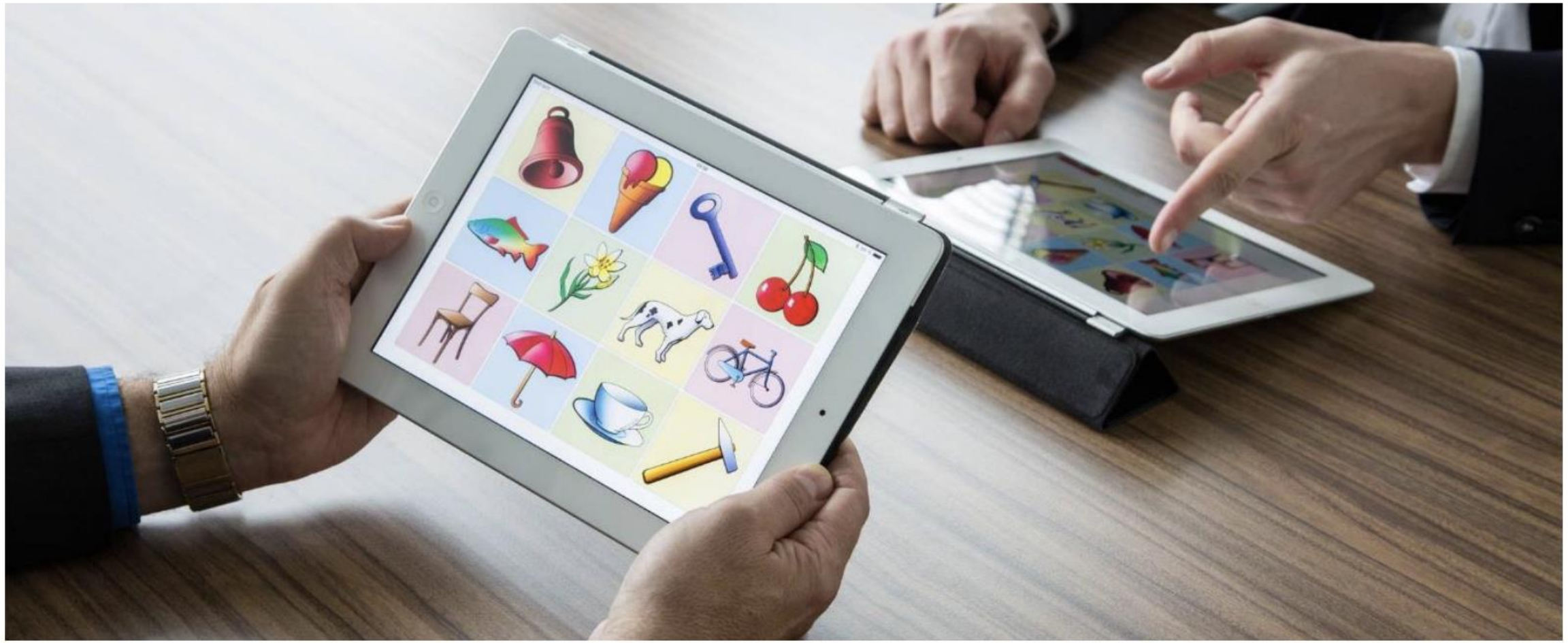


Architektur

Verschlüsselung

Ausblick

Syndromkurztest (SKT)



Aufbau

Subtest I: Gegenstände benennen und einprägen

Aufbau

Subtest II: Gegenstände unmittelbar reproduzieren

Aufbau

Subtest III:
Zahlen
lesen

Aufbau

Subtest IV: Zahlen ihrer Größe nach ordnen

Aufbau

Subtest V: Zahlen zurücklegen

Aufbau

Subtest VI: Symbole zählen

Aufbau

Subtest VII: Interferenz-test

Aufbau

Subtest VIII: Gegenstände mittelbar reproduzieren

Aufbau

Subtest IX: Gegenstände wieder-erkennen

Subtest I: Gegenstände benennen und einprägen (A)

- Vorlagentafel mit alltäglichen Gegenständen
- Proband benennt Gegenstände laut und prägt sich diese gleichzeitig ein
- Zeit zur Benennung und Einprägung wird protokolliert

(A) = Aufmerksamkeit

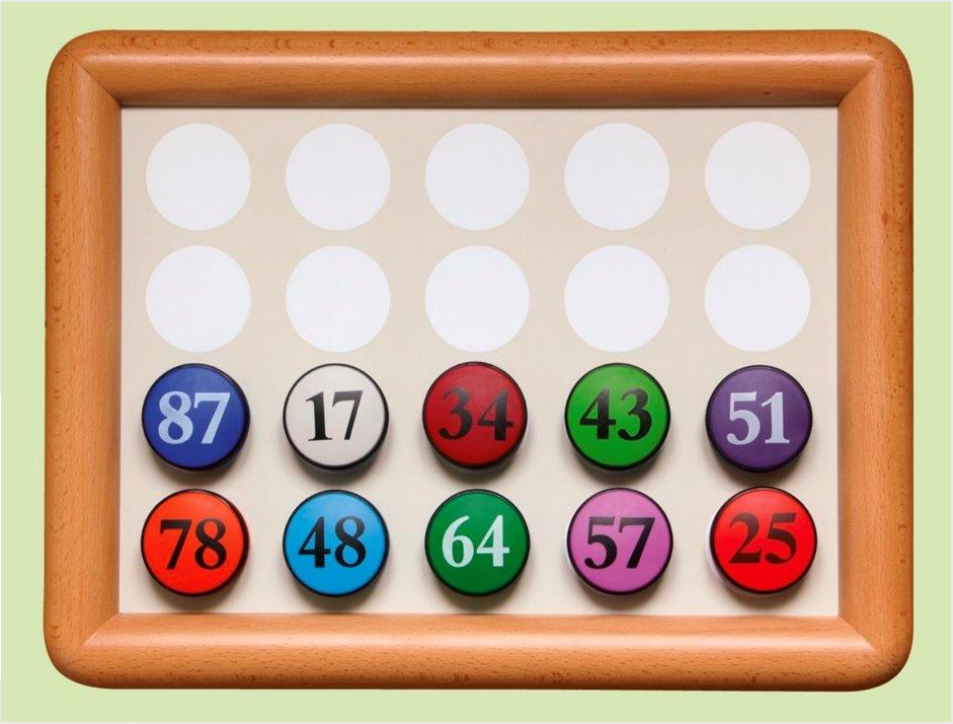
Subtest II: Gegenstände unmittelbar reproduzieren (G)

- Im Anschluss von Subtest I so viele Gegenstände wie möglich zu reproduzieren
- Vorzeitige Beendigung nur wenn Proband alle zwölf Gegenstände vor Ablauf der Zeit aufgelistet hat

(G) = Gedächtnis

Subtest III: Zahlen lesen (A)

- Zahlen müssen nicht eingeprägt werden
- Zweistellige Zahlen, die auf dem Stein als auch auf dem Feld, wo sie liegen, stehen
- Probanden lesen die Zahlen nach Leserichtung laut vor
- Benötigte Zeit wird protokolliert



(A) = Aufmerksamkeit

Subtest IV: Zahlen ihrer Größe nach ordnen (A)

- Zahlen ihrer Größe nach beginnend mit der kleinsten Zahl sortieren
- Benötigte Zeit wird protokolliert

(A) = Aufmerksamkeit

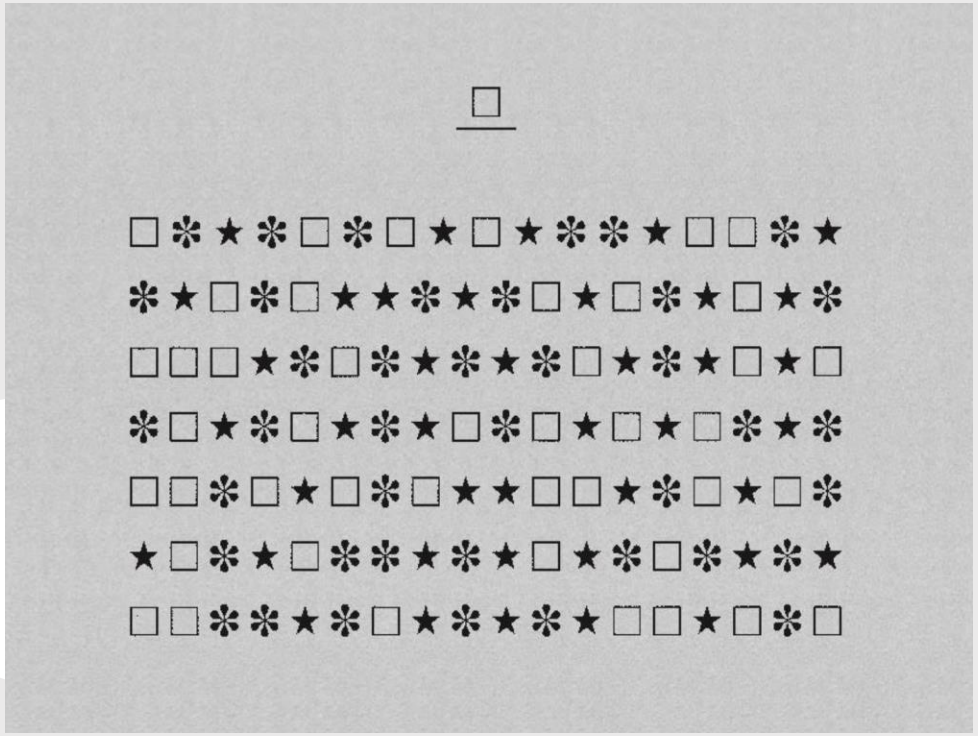
Subtest V: Zahlen zurücklegen (A)

- Zahlen auf ihren ursprünglichen Platz zurücklegen
- Stein mit der Nummer 17 zurück auf das Feld mit der Nummer 17

(A) = Aufmerksamkeit

Subtest VI: Symbole zählen (A)

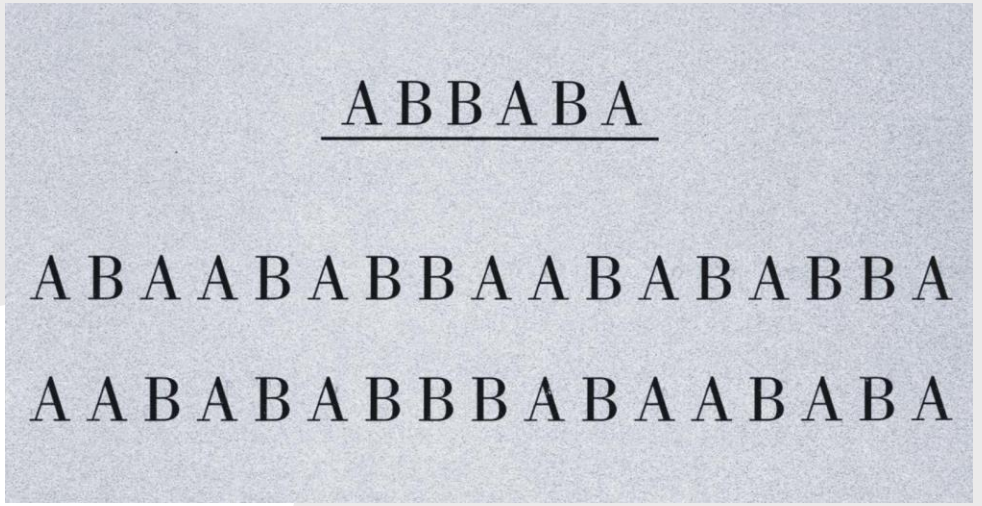
- Tafel mit unterschiedlichen Symbolen
  - SKT Form A: Quadrate, Sterne und Schneeflocken
- Proband soll nur die Quadrate so schnell wie möglich zählen
- Obere unterstrichene Quadrat dient als Beispiel und nicht Teil des Subtests
- Anzahl der Quadrate sowie benötigte Zeit wird protokolliert



(A) = Aufmerksamkeit

Subtest VII: Interferenztest (A)

- Anspruchsvollster Test
- Tafel mit willkürlicher Abfolge zweier Buchstaben
  - SKT Form A: A und B
- "B" sagen, wenn man "A" liest und umgekehrt
- Oberste Zeile dient nur als Beispiel und nicht Teil des Subtests



(A) = Aufmerksamkeit

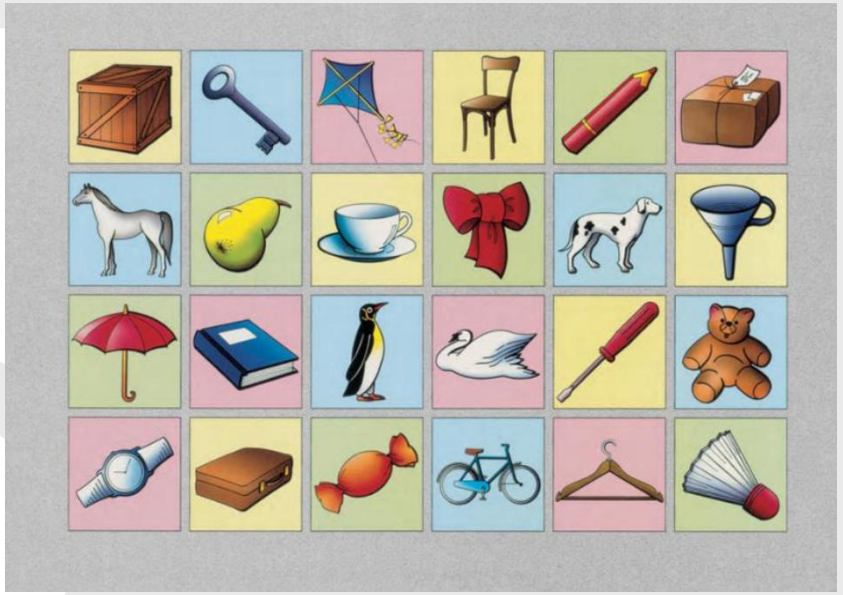
Subtest VIII: Gegenstände mittelbar reproduzieren (G)

- Alle Gegenstände aus Subtest I laut zu nennen
- Test wird nur vorzeitig beendet wenn der Proband sich an alle Gegenstände erinnern kann
- Anzahl der fehlenden Gegenstände wird protokolliert
- Falschnennungen werden bei Wiederholung als korrekt gewertet
- Konfabulationen werden lediglich notiert

(G) = Gedächtnis

Subtest IX: Gegenstände wiedererkennen (G)

- Bildertafel mit 48 Gegenständen vorgelegt
- Die zwölf aus Subtest I herauszusuchen und laut zu benennen
- Test wird nur vorzeitig beendet, wenn alle Gegenstände erkannt wurden
- Konfabulationen werden lediglich ignoriert
- Falschnennungen werden bei Wiederholung als korrekt gewertet

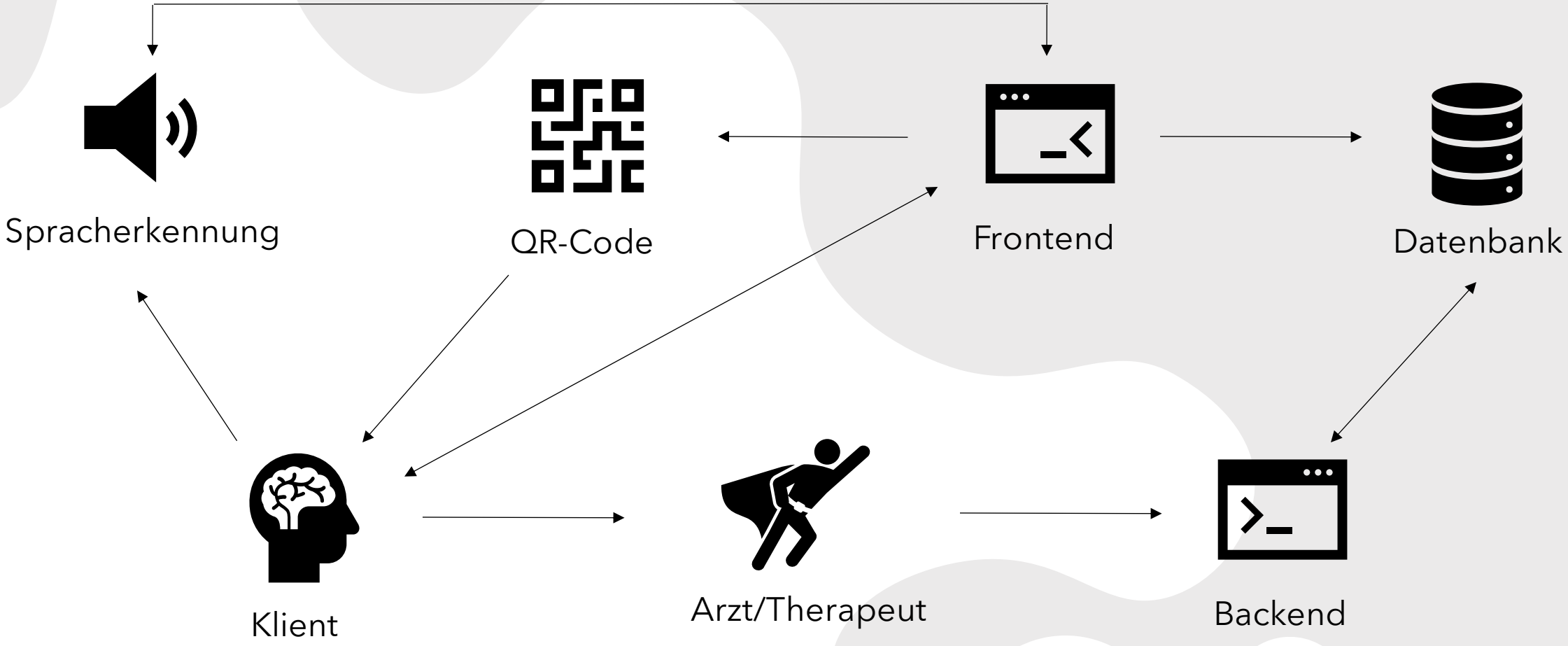


(G) = Gedächtnis

Demo

- Einblick in den aktuellen Stand des SKT Tests sowie zur Verschlüsselung

Architektur



Technologie

Vue.js

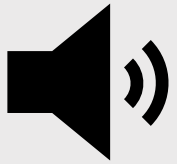
Python

Docker

MongoDB

Flask

Spracherkennug



- JavaScript Speech Recoginition API
- Definierte Synonyme für jeden Gegenstand
- Abgleich mit Hilfe der Levenshtein-Distanz
- "Dauerhafte" Spracherkennung

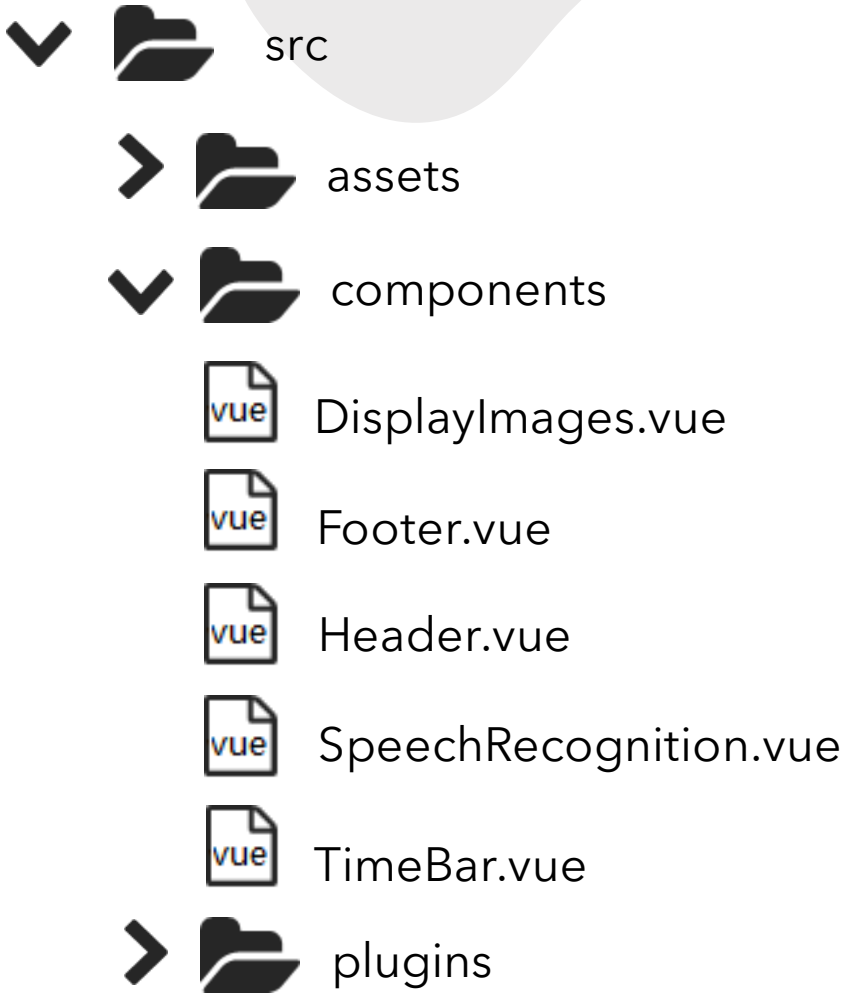
Ordnerstruktur

- src
  - assets
  - components
  - plugins
  - views
  - store
  - router
  - App.vue
  - Main.js

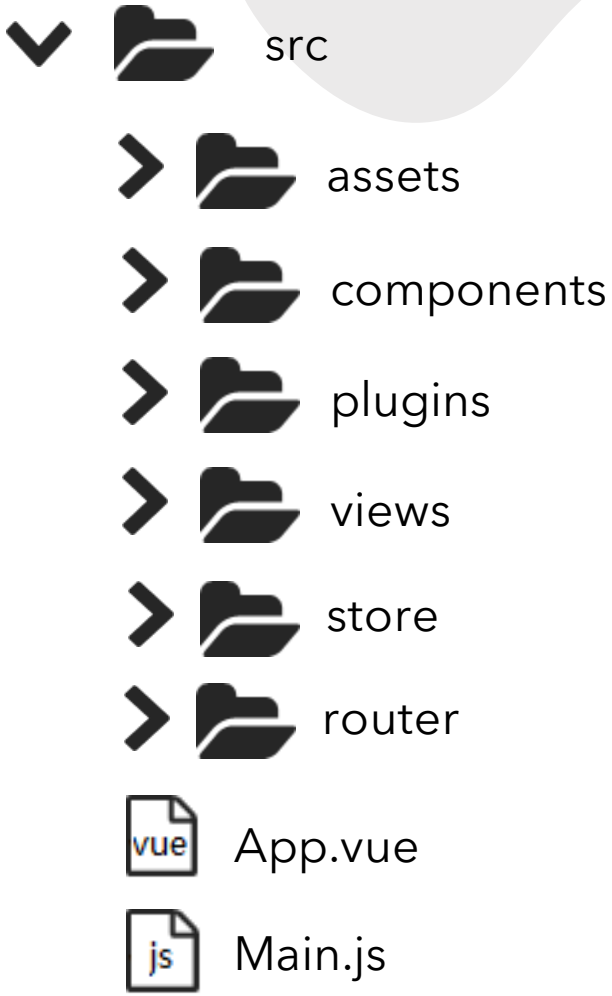
Ordnerstruktur

- src
  - assets
    - images
      - ballon.jpg
      - banane.jpg
      - ...
    - style
      - Bootstrap-vue
      - Style.css

Ordnerstruktur



Ordnerstruktur



Ver- und Entschlüsselung

- Personenbezogene Gesundheitsdaten bedürfen besonderen Schutz
- Zusätzlich zu TSL
- Symmetrische Verschlüsselung
  - Klient erhält symmetrischen Schlüssel als QR-Code
  - Zugang der Daten nur mit Einwilligung des Klienten
- Asymmetrische Verschlüsselung
  - Privater Schlüssel nur im für Auswertung vorgesehenen Institut

Ver- und Entschlüsselung

- Symmetrische Verschlüsselung
  - AES-GCM
- Asymmetrische Verschlüsselung
  - RSA-OAEP
- Genutzte Library: SubtleCrypto - WebApi

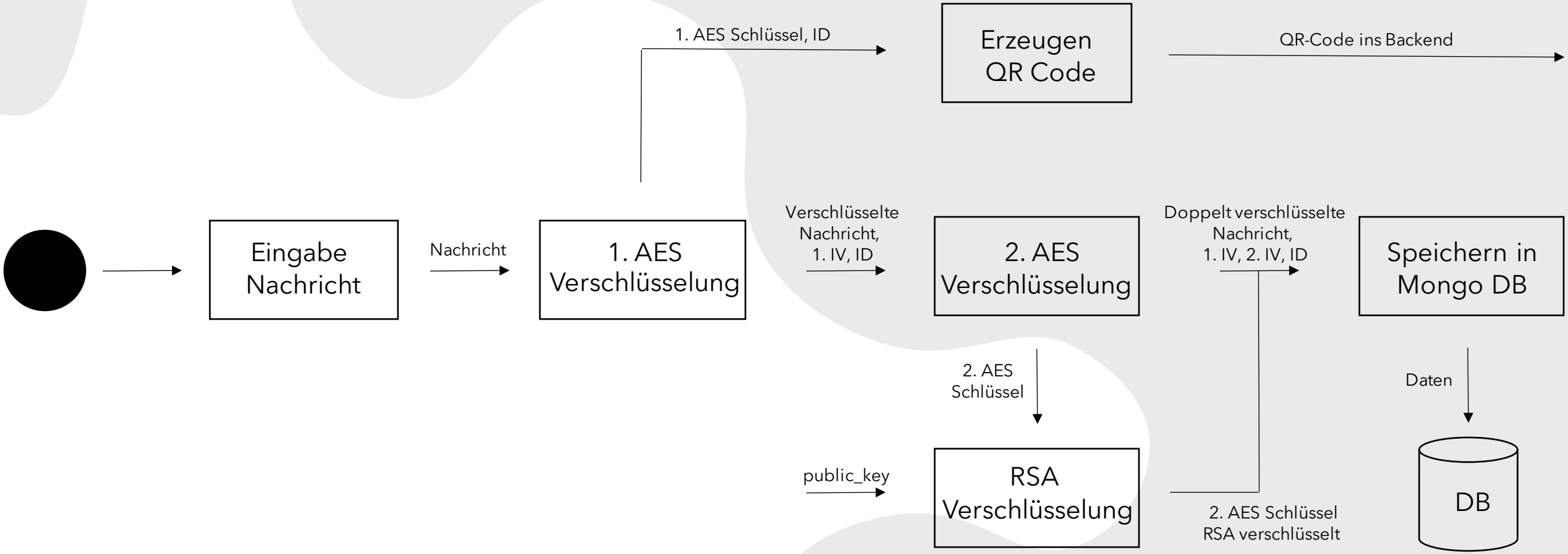
Advanced Encryption Standard (AES)

- Symmetrisches Verschlüsselungsverfahren d.h. Schlüssel zum Ver- und Entschlüsseln sind identisch
- Schlüssellänge 256 Bit
- Pragmatisch sicher: Nur mit unrealistischem Aufwand zu brechen
- AES-GCM: Galois Counter Mode ermöglicht Verschlüsselung beliebig langer Nachrichten

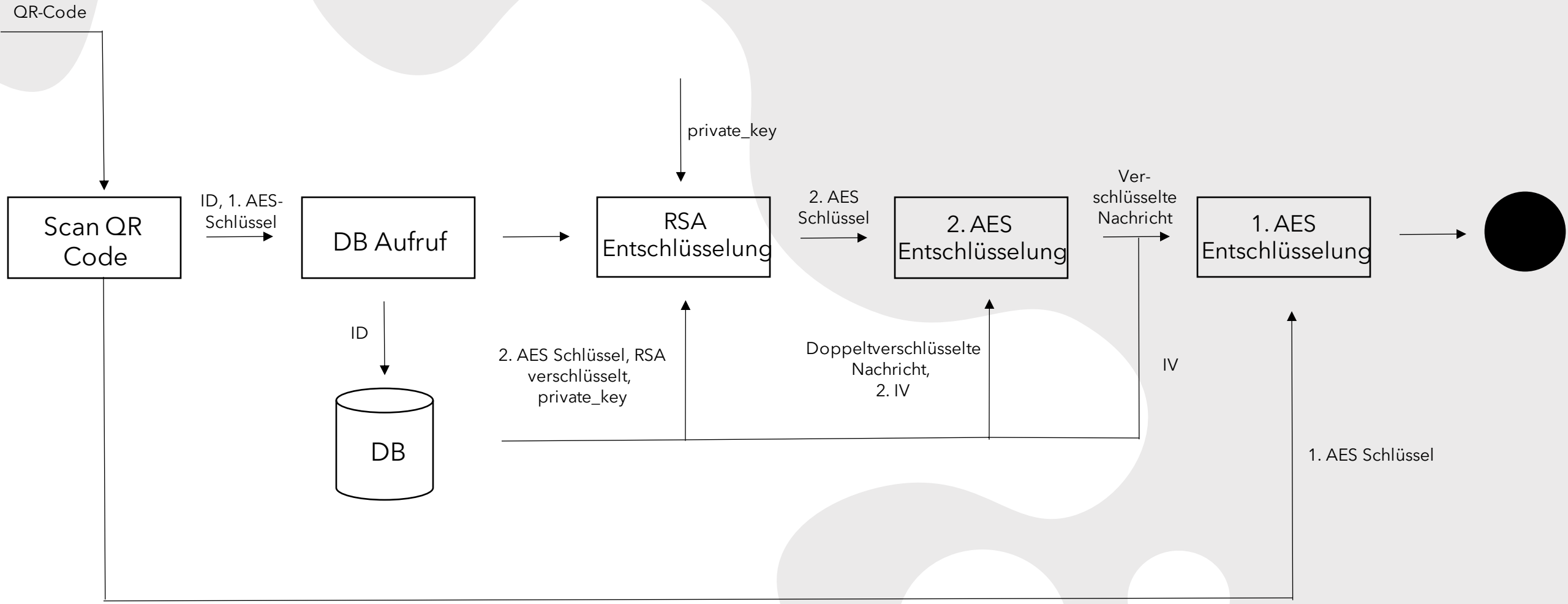
Rivest-Shamir-Adleman (RSA)

- Asymmetrisches Verschlüsselungsverfahren
- Schlüssellänge 2048 Bit
- In Kombination mit Paddingverfahren: Optimal Asymmetric Encryption Padding
- => RSA-OAEP
- Langsam und begrenzte Länge der Nachricht
- Verschlüsselung des symmetrischen Schlüssels mit RSA-OAEP

Frontend


1. AES Schlüssel, ID
Erzeugen QR Code
QR-Code ins Backend
Eingabe Nachricht
Nachricht
1. AES Verschlüsselung
Verschlüsselte Nachricht, 1. IV, ID
2. AES Verschlüsselung
Doppelt verschlüsselte Nachricht, 1. IV, 2. IV, ID
Speichern in Mongo DB
2. AES Schlüssel
Daten
public_key
RSA Verschlüsselung
DB
2. AES Schlüssel RSA verschlüsselt

Backend


QR-Code
Scan QR Code
ID, 1. AES-Schlüssel
DB Aufruf
ID
DB
private_key
RSA Entschlüsselung
2. AES Schlüssel, RSA verschlüsselt, private_key
2. AES Schlüssel
2. AES Entschlüsselung
Doppeltverschlüsselte Nachricht, 2. IV
Ver-schlüsselte Nachricht
IV
1. AES Entschlüsselung
1. AES Schlüssel

Ausblick

- Umsetzung aller Subtests
- Verbesserung des Frontend Designs
- Fehlerbehandlung
- Audio Recording
- User-Anmeldung (Patientendaten: Namen, Geburtstag)
- Webinterface zur Entschlüsselung