ROBERT KOCH INSTITUT

Grundlagen der “Corona-App”

V 0.1.1 20200513 Bonn * Jochim Selzer js@crypto.koeln
6AA4 89F9 9E1F DCBA FF00 F291 8A97 4A5C 0970 E0CF

Worum geht es?

- Es geht um
  - was die Corona-App leisten kann,
  - was nicht,
  - und warum
- Es geht nicht um
  - eine Toolsdiskussion

Was ich will vs was ich fordere

- Ich will: mich nicht anstecken
- Ich fordere: eine App

Was bisher geschah

- 23.3.: So ringt die GroKo um die Verwendung von Handydaten
- 1.4.: Heinrich-Hertz-Institut: Europäische Corona-Tracking-App in Entwicklung
- 19.4.: Corona-Tracing-App: Absetzbewegungen beim multinationalen Projekt PEPP-PT
- 24.4.: Corona-App: Apple und Google wollen Regierungswünschen nachkommen
- 26.4.: Dezentrale Lösung: Bundesregierung sattelt bei Corona-Tracing-App radikal um

Alle entwickeln vor sich hin

- Australien führt freiwillige Corona-App ein – Vorbild war Singapur
- TraceTogether: Singapur plant Öffnung der staatlichen Coronavirus-Tracking-App
- Stopp-Corona-App: Österreich will Vorzeigemodell für Europa schaffen
- Frankreich will von Apple Zugeständnisse für Corona-App
- Coronavirus: Eine App entscheidet in China über Quarantäne

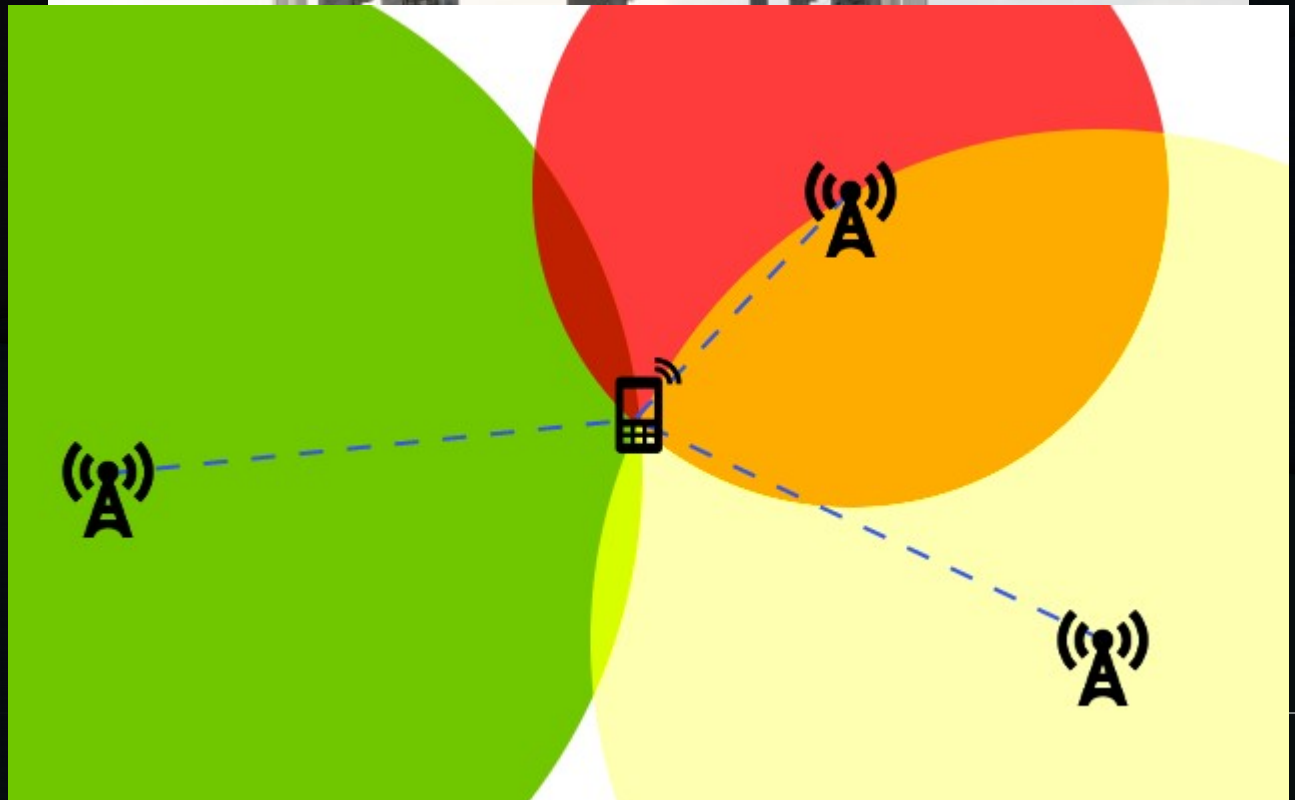
Aber da gibt’s doch was vom RKI

- Kein Contact-Tracing
- Mehrere Schwachstellen:
  - Ruft die Daten nicht vom Armband, sondern vom Online-Account ab
  - Verwirft OAuth-Tokens nicht
  - Pseudonymisierung erst beim RKI

Ansatz 1: Alle ständig überwachen

- Alle Smartphones senden ständig ihre GPS-Koordinaten
- Nachteile:
  - unpräzise
  - rechtsstaatlich problematisch

Idee: Funkzellenabfrage



Funkzellenabfrage

- Vorteile:
  - Daten sind automatisch vorhanden.
  - Funktioniert unabhängig vom Telefonmodell
- Nachteil:
  - Unpräzise, für Unterschreitung des Infektionsabstands ungeeignet

Verfeinerung: WLAN-Ortung

- Nutzt die bekannten Standorte von WLAN-Routern
- Vorteil: präziser, weil geringere Reichweite
- Nachteile:
  - Telefone müssen WLAN aktiviert haben.
  - Apple und Google müssen kooperieren

Neue Aufgabe

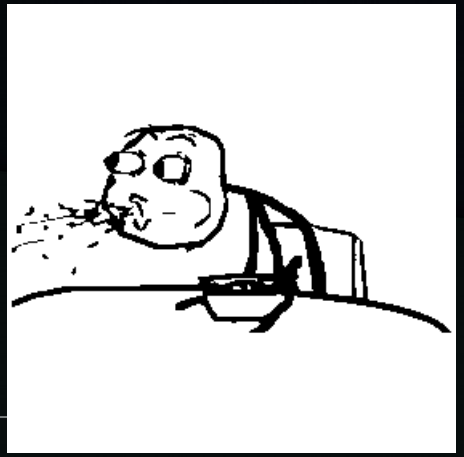
- Wird eine Person positiv getestet, beginnt eine mühevolle, fehlerträchtige, manuelle Suche nach allen Kontakten dieser Person in den letzten Tagen
- Idee: automatische Erfassung der Kontakte
- Wichtig: Dieses Verfahren schützt nicht mich vor einer Infektion, sondern warnt nur andere vor mir.
- Problem: Wie soll das ohne Totalüberwachung funktionieren?

Ansatz 2: Kontakte nachverfolgen

Idee: Es kommt nicht auf den genauen Standort einer Person an, sondern nur darauf, ob sie einer infizierten Person zu lange zu nahe kam.

Idee: Ultraschall

- Versuch in Österreich
- Funktioniert im Bereich von 1,5 m
- Schwierigkeiten:
  - nicht mehrere Smartphones gleichzeitig
  - Hüllen und Taschen dämpfen den Schall
  - Mikrofon muss freigeben werden
- Ergebnis: 4 % Installationsquote



Idee: Bluetooth

- Bluetooth funktioniert nur auf relativ kurze Distanz.
- Messung von
  - Empfangspegel (RSSI)
  - Sendeleistung (Tx Power)
  - Empfangsempfindlichkeit (Rx Power)
  - Laufzeit
  - Ausrichtung, Bildschirmstatus

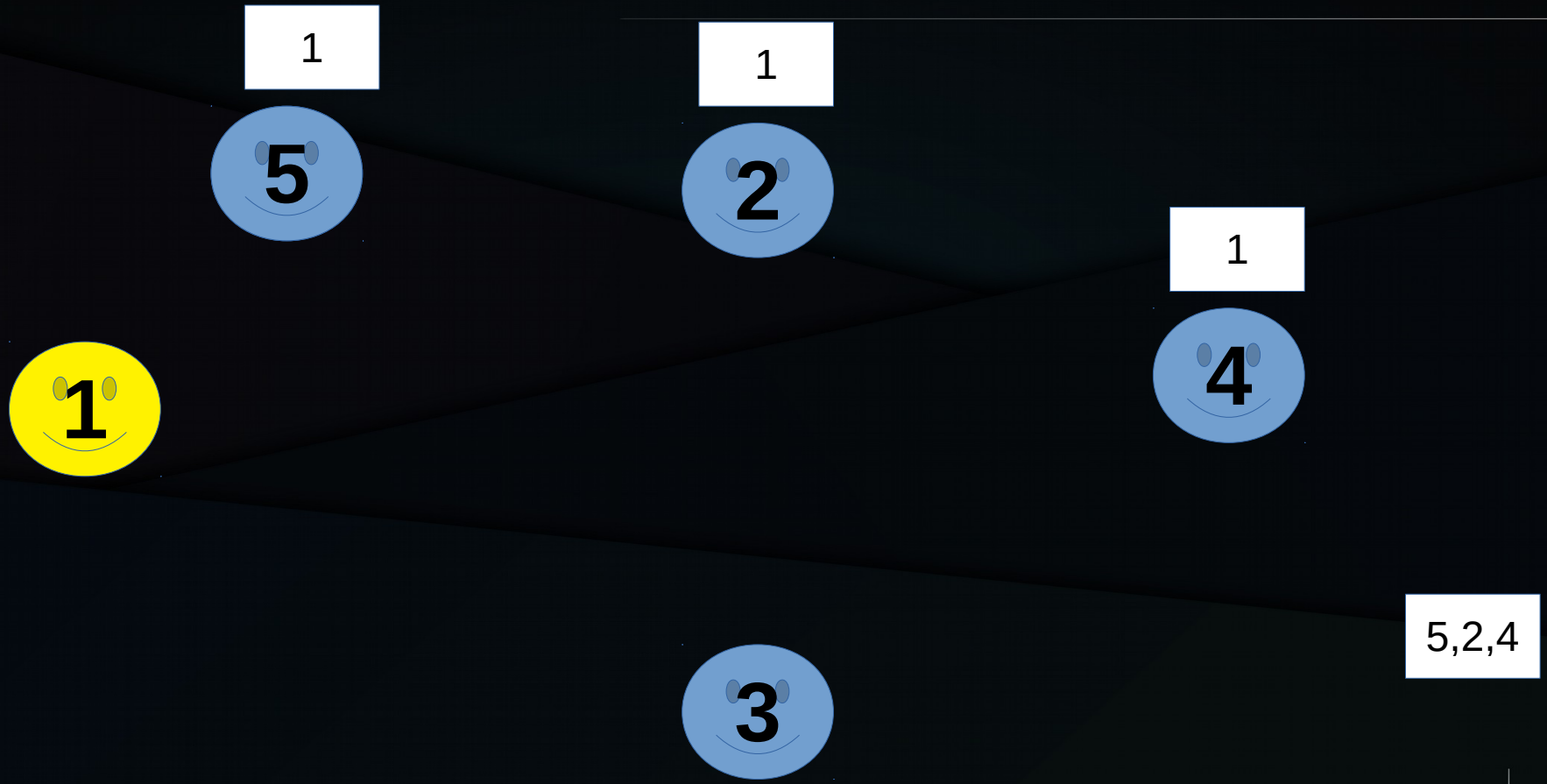
Schwierigkeiten der Methode

- Kaum praktische Erfahrungen mit Entfernungsbestimmung per Bluetooth
- Wände lassen Bluetooth durch, aber keine Viren
- Tests bei der Bundeswehr lieferten bis zu 18 % falsch positiv (und das ohne Wände und Scheiben)
- Das Signal kann um Ecken reflektiert werden
- Sende- und Empfangscharakteristiken abhängig von Smartphone-Modell und wie es gehalten wird
- Android und iOS liefern an die Apps bislang nur übertragene Datenpakete, keine Signalstärken
- Die iOS-App müsste ständig im Vordergrund laufen

Technische Lösungen

- Google und Apple entwickeln ein API
- Die Annäherungsdaten werden auf Betriebssystemebene gesammelt, eine App muss sie nur noch abfragen und auswerten (lassen)
- PEPP-PT (Pan European Privacy Protecting Proximity Tracing)
- DP3T (Decentralized Privacy-Preserving Proximity Tracing)

IDs sammeln



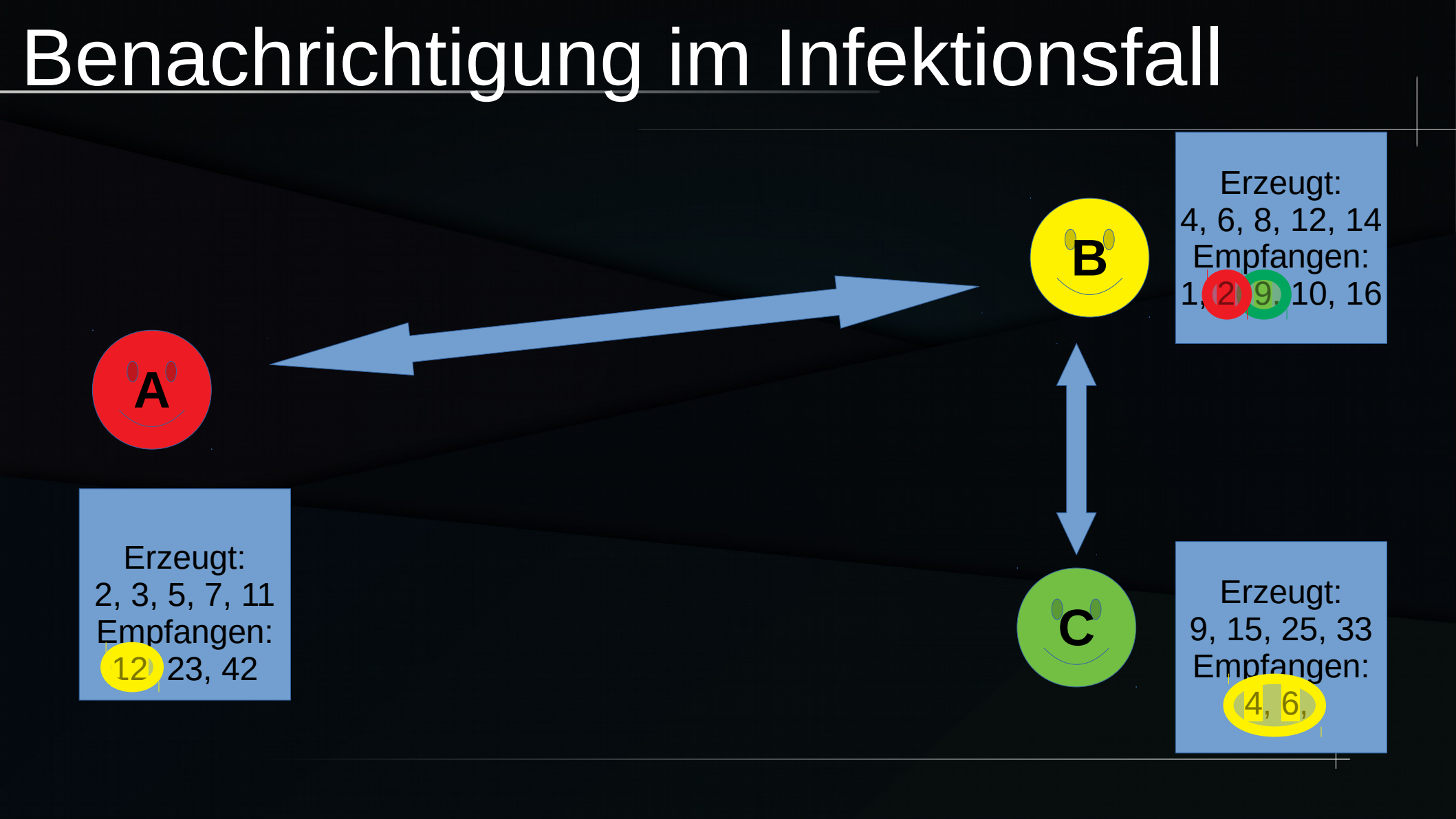
Erster Stolperstein

- Das Smartphone sendet ständig die gleiche ID.
- Lösung: Die ID wechselt regelmäßig.

Wenn ich positiv getestet werde

- Alle haben auf ihren Telefonen eine Liste von IDs,
  - denen sie begegnet sind
  - die sie erzeugt und verteilt haben
- Die infizierte Person veröffentlicht die Liste der von ihr erzeugten IDs
- Alle sehen nach, ob eine dieser IDs in ihrer Empfangsliste auftaucht.

Benachrichtigung im Infektionsfall



Weitere Probleme

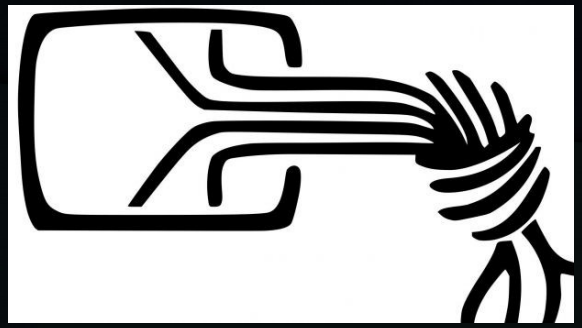
- Funktioniert angeblich nur bei 60 % Akzeptanz der Leute insgesamt.
- Nur 70 % haben überhaupt ein Smartphone, also müssen 86 % der Besitzerinnen die App installieren.
- Bei Android müssen die Smartphonehersteller kooperieren (Google will bis Android 6 vom Oktober 2015 ausliefern)
- Große Spannbreite beim Infektionszeitraum führt zu Fehlalarmen
- Hoher Zeitdruck führt zu Fehlern (siehe RKI-App)
- “Freiwilligkeit”, “Anreize schaffen”

Noch mehr Probleme

- Wie verhindere ich mutwillig falsche Krankmeldungen? (Freischaltschlüssel der Ärztin, Telefonnummer hinterlassen)

10 Prüfsteine des CCC

I. Gesellschaftliche Anforderungen
   1) Epidemiologischer Sinn & Zweckgebundenheit
   2) Freiwilligkeit & Diskriminierungsfreiheit
   3) Grundlegende Privatsphäre
   4) Transparenz & Prüfbarkeit



10 Prüfsteine des CCC

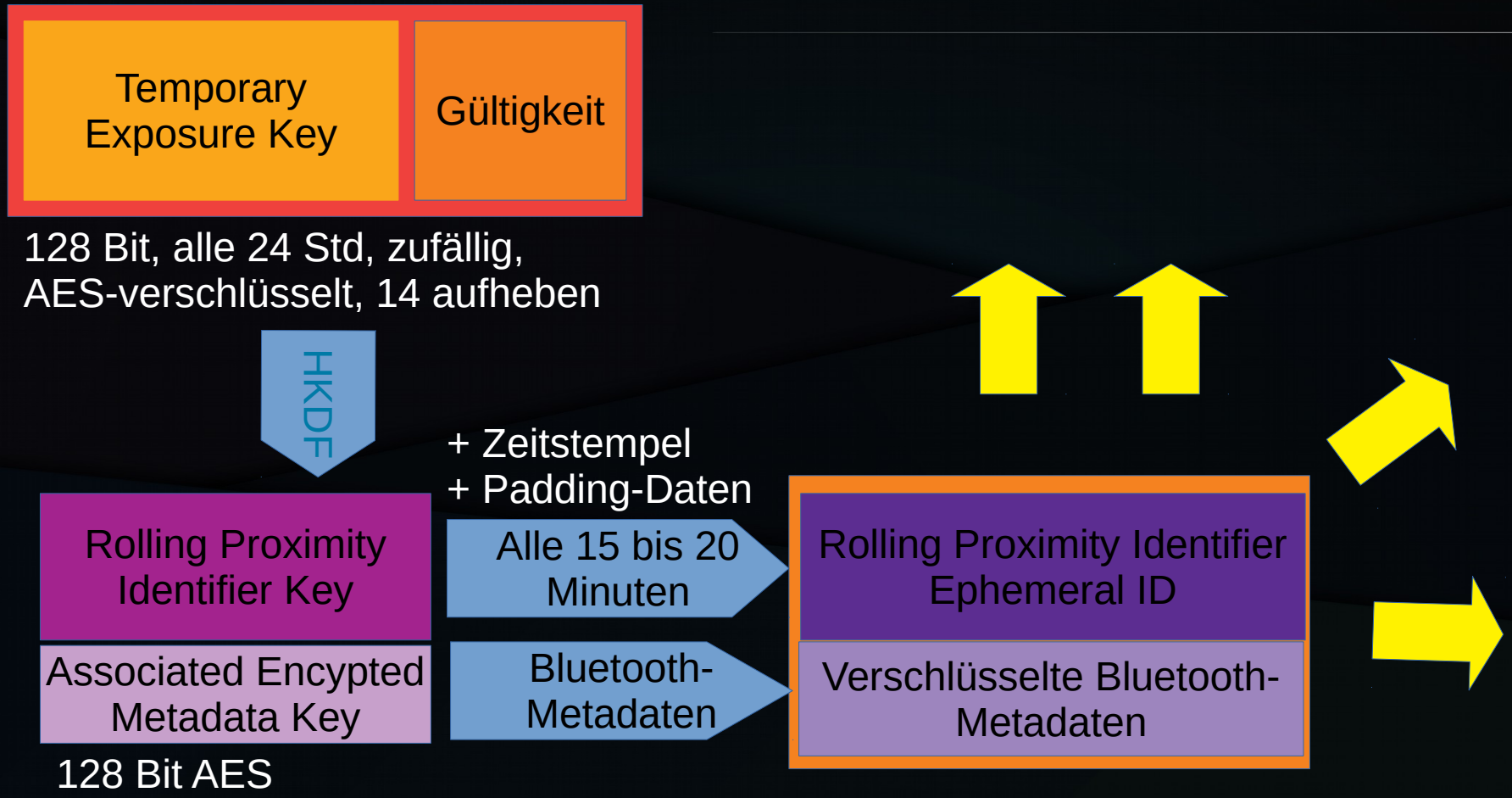
II. Technische Anforderungen

5) Keine zentrale Entität, der vertraut werden muss
6) Datensparsamkeit
7) Anonymität
8) Kein Aufbau von zentralen Bewegungs- und Kontaktprofilen
9) Unverkettbarkeit
10) Unbeobachtbarkeit der Kommunikation

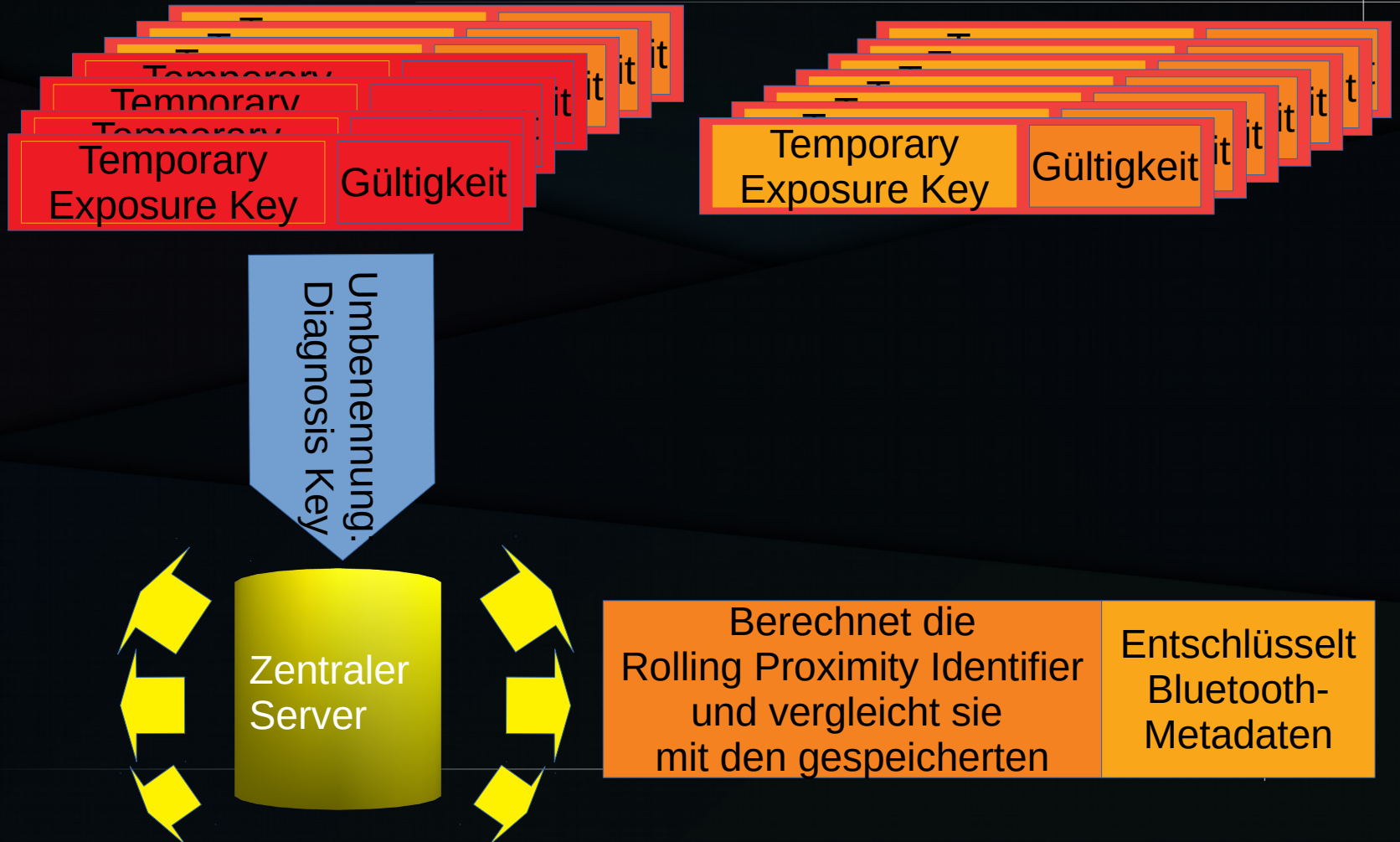
Zentral vs dezentral

- Zentral: Alle Annäherungsdaten werden an einen zentralen Server geschickt, der sie auswertet und Infektionswarnungen verschickt.
  - Vorteil: Tuning relativ leicht möglich
  - Nachteil: Ich muss einer zentralen Instanz vertrauen
- Dezentral: Alle Daten verbleiben auf dem Smartphone. Ein zentraler Server wird nur als Relay zum Versenden einer Warnung genutzt.
  - Vorteil: Ich muss nur meinem Smartphone vertrauen.
  - Nachteile:
    - Tuning ist komplizierter.
    - Deanonymisierung bei Veröffentlichung der Infektionsdaten eventuell möglich

Schlüsselerzeugung auf dem Gerät



Bei positiver Diagnose



Warum dauert das alles so lange?

- Präzise Abstandsmessung per Bluetooth ist nicht trivial.
- Die Bundesregierung setzt auf etablierte Unternehmen wie Telekom und SAP.
- Große Unternehmen sind tendenziell langsamer als kleine Startups.
- Die öffentliche Hand hat tendenziell Pech mit Großprojekten (BER, Elbphilharmonie, LKW-Maut, Expo 2000).
- Geplant ist ein Rollout auf 48 Mio Geräte. Entsprechend groß ist die Angriffsfläche, wenn etwas schiefgeht.

Fragen und Einwände

- Apple und Google sind böse (aber deren Telefone habe ich dennoch gekauft)
- Ich habe kein Google-Konto, nutze Lineage (ungelöst)
- Komme ich leichter an einen Test, wenn ich eine Kontaktwarnung erhalten habe?
- Soll die App auch die Quarantäne überwachen?

Fazit

- Wir wissen nicht, ob und wie gut die App funktionieren wird.
- Sie wird auf jeden Fall nur ein Baustein, kein Allheilmittel sein.
- Entscheidend wird sein, dass wir ihr vertrauen können.