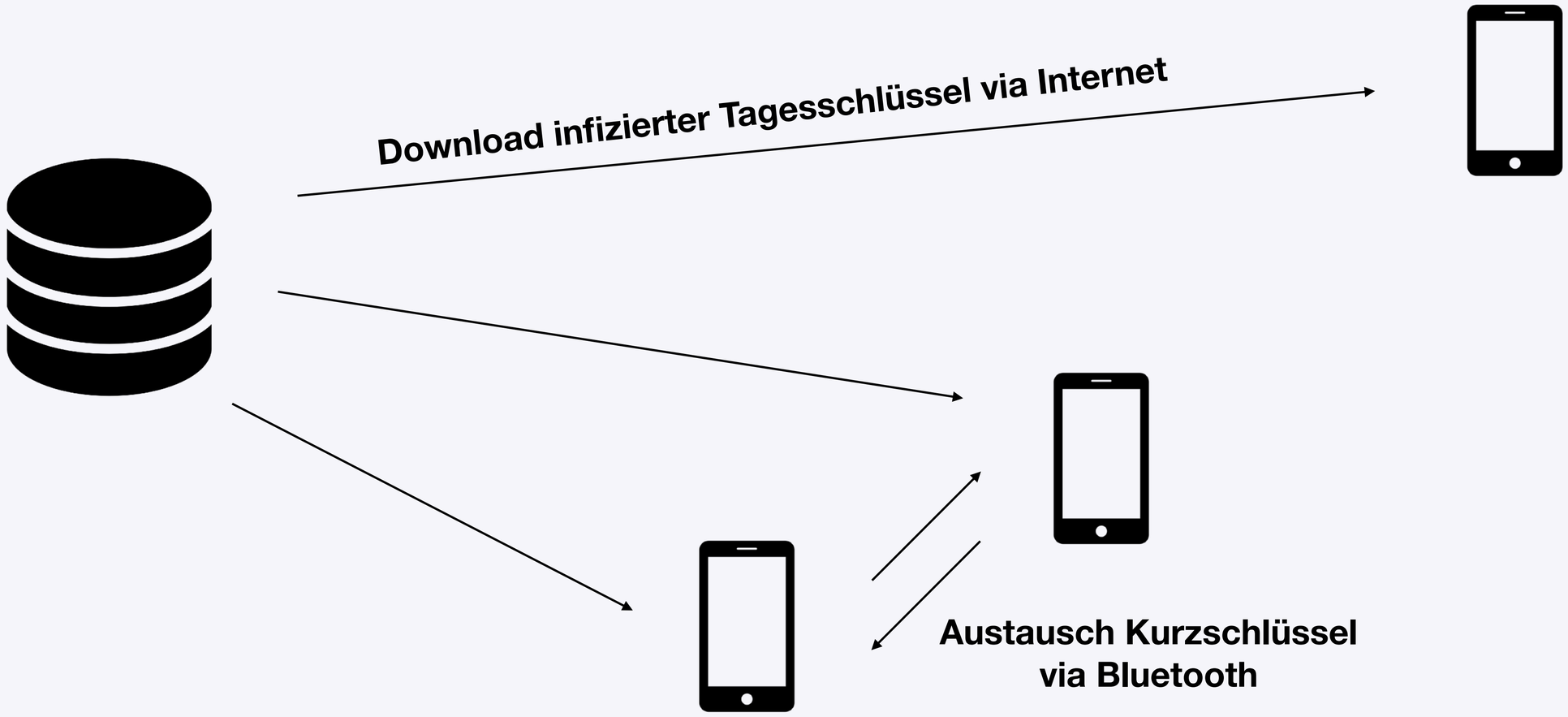
TECHNIK DER CORONA-WARN-APP

HENNING TILLMANN, D64

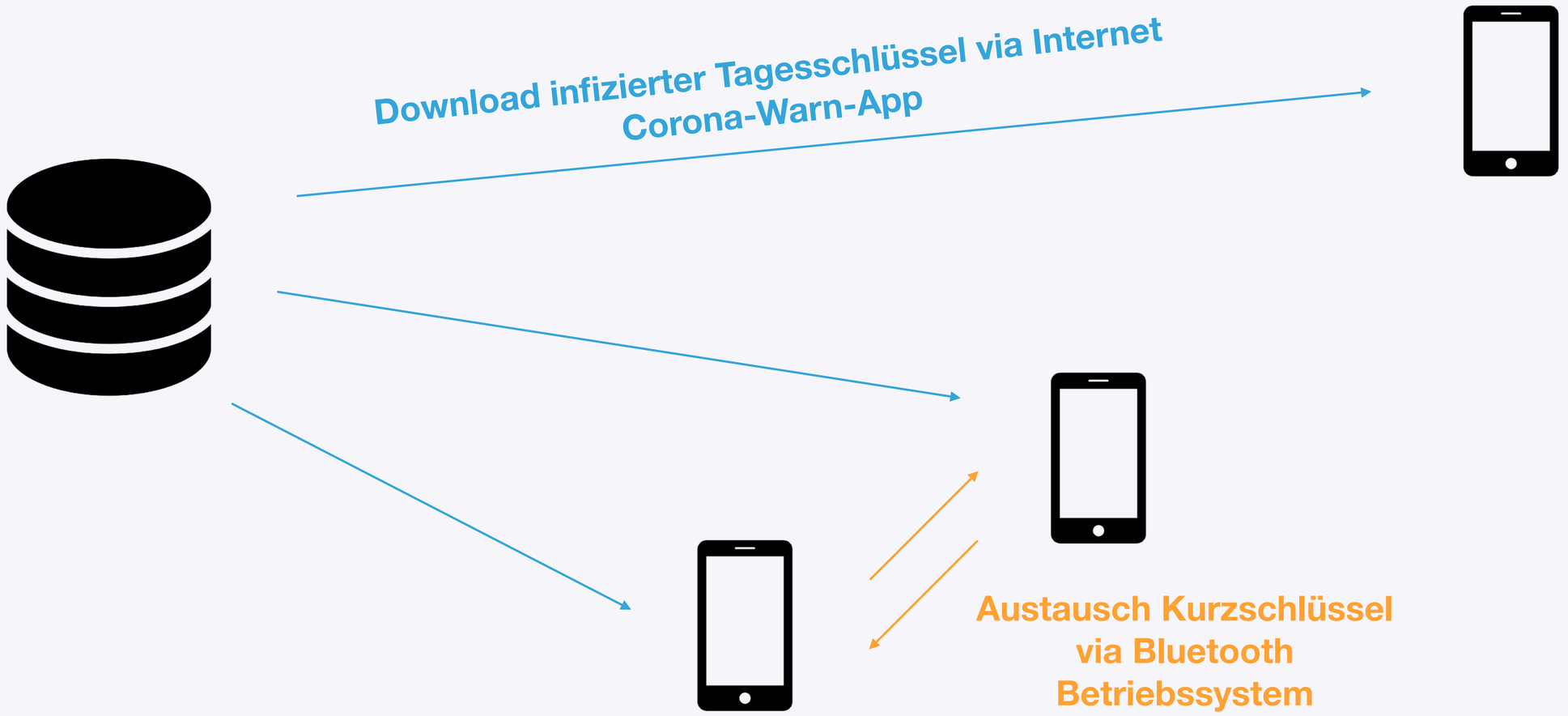
D64
Zentrum für
Digitalen Fortschritt

AUSTAUSCH SCHLÜSSEL



D64
Zentrum für
Digitalen Fortschritt

AUSTAUSCH SCHLÜSSEL

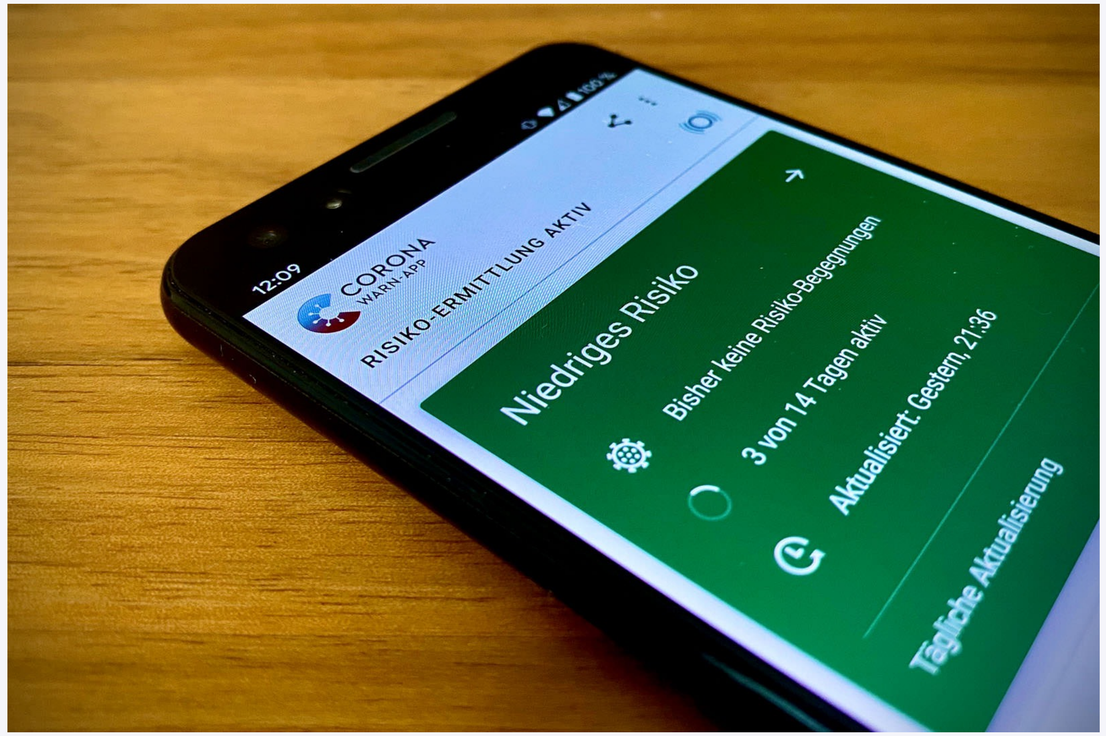


D64
Zentrum für
Digitalen Fortschritt

DEZENTRALER ANSATZ

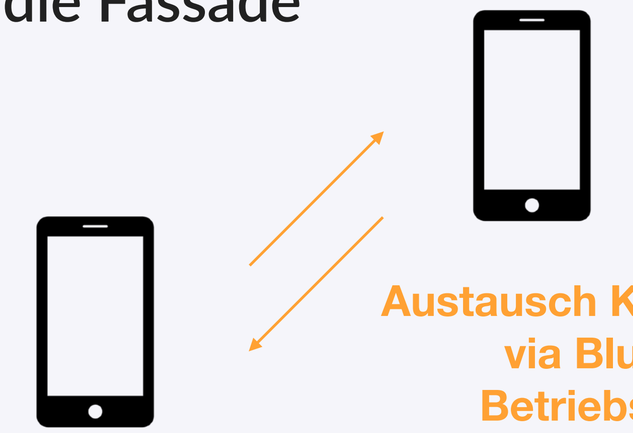
- Verfahren des Apple/Google-Frameworks kryptografisch clever, aber auch nicht direkt einfach verständlich.

- Erläuterung im Pinned Tweet auf Twitter-Profil @henningtillmann.



ROLLE APPLE/GOOGLE

- Grundlage der CWA ist Exposure Notification Framework von A+G, im Frühling veröffentlicht.
- Hauptarbeit des Tracing übernimmt EN-Framework.
- Fast alle westlichen Länder mit Corona-App verwenden das Framework.
- Funktionalität aller Corona-Apps mit dem Framework fast alle identisch.
- Einfach ausgedrückt:
  Framework ist das Fundament
  CWA ist die Fassade



D64
Zentrum für
Digitalen Fortschritt

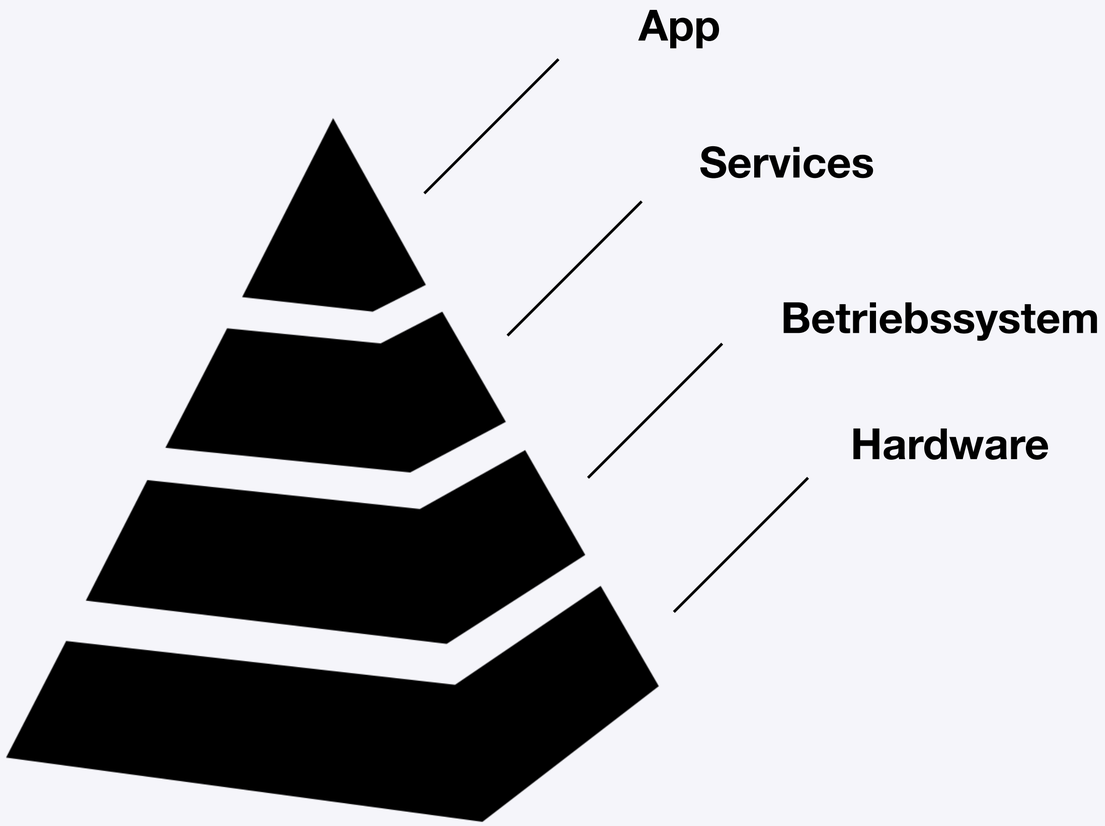
PRINZIP EN-FRAMEWORK

- Wenn sich zwei Geräte treffen, werden Kurzschlüssel ausgetauscht und Signalstärke vermerkt
- Betriebssystem protokolliert die Zusammentreffen, übernimmt Matching
- Nutzung von GPS, o.ä. ausgeschlossen

- Was macht die CWA überhaupt noch?
  - Design
  - Herunterladen der Tagesschlüssel
  - Kann Risikoermittlung etwas beeinflussen
  - Verfahren für Positiv-Meldung

WARUM NICHT OHNE APPLE/GOOGLE?

- Wenn Bluetooth-Ansatz ohne Apple/ Google, muss Schlüsselaustausch durch App übernommen werden.
  - Extrem unzuverlässig, beim iPhone muss App bspw. permanent im Vordergrund sein.
  - Frankreich, Australien, … gescheitert.



D64
Zentrum für
Digitalen Fortschritt

ABER ASIEN!

- Asiatische Digitalstrategien grundsätzlich anders als in westlichen Ländern, nicht vergleichbar mit Bluetooth Corona-Warn-App.
- Komplette digitale Erfassung bestimmte Lebensbereiche (auch Kreditkartenabbuchungen).
- Tracing- (eher Tracking-)Apps verwenden GPS. Durch Nutzung von GPS erhalten Apps mehr Möglichkeiten.
- Einfach ausgedrückt: GPS-Apps haben im Hintergrund mehr Möglichkeiten. Zeichnen aber auch permanent Bewegungsmuster auf.

KEINE UPGRADES MÖGLICH?

- Doch!
  - Alles was nichts mit dem Schlüsselaustausch zu tun hat:
    Corona-Warn-App (Telekom/SAP), z. B. Kontakttagebuch, Einbindung Infos (Dashboard, Verordnungen).
  - Alles was mit Schlüsselaustausch zu tun hat:
    Apple/Google, z. B. automatische Clustererkennung, Erfassung Zeitpunkt.

- Aber:
  - Grundprinzip des dezentralen Ansatzes lässt sich – außer mit sehr viel Druck auf Apple/Google – nicht durch Erweiterungen ändern.
  - Dilemma: Will man das Grundprinzip verlassen, entsteht eine nicht funktionierende App.

DANKE!

@henningtillmann
@d64ev