

# Corona Warn App

Printout von [blog.jakobs.systems](https://blog.jakobs.systems)

Tomas Jakobs

27 April 2021

## Inhaltsverzeichnis

<b>Blog-Serie in drei Teilen</b>	<b>3</b>
Eine Frage der Prioritäten . . . . .	4
Nun sag, wie hast Du's mit Open Source? . . . . .	5
Grundannahmen . . . . .	6
Abstandsmessung . . . . .	7
Messung der Dauer . . . . .	9
Differenzen und Unsicherheiten . . . . .	10
Aufbau der Gesamtlösung . . . . .	10
<b>Teil II - in the meantime</b>	<b>13</b>
Fortsetzung: Aufbau der Gesamtlösung . . . . .	14
Der Schlüsselmeister in der Matrix . . . . .	16
Komplexität . . . . .	18
Komfortfunktionen vs. Corona . . . . .	20
<b>Teil III - in the meantime</b>	<b>21</b>
App ist nur ein Baustein . . . . .	21
Abnormale User-Stories . . . . .	22
Ist jemand krank? . . . . .	22
Bewerbungsgespräch . . . . .	22
Die Verhinderung . . . . .	22
Der Systemgegner . . . . .	23
Der Bart-Simpson-Typ . . . . .	23
Function Creeping . . . . .	23
Daten vs. Selbstbelastungsfreiheit . . . . .	24
Was ist ein Leben wert? . . . . .	25
Es gibt Wichtigeres als Apps . . . . .	25
Ein Wettrüsten beginnt . . . . .	27
<b>Änderungsverzeichnis</b>	<b>28</b>
Update 20.05.2020 . . . . .	28
Update 23.05.2020 . . . . .	28
Update 30.05.2020 . . . . .	28
Update 13.08.2020 . . . . .	28
Update 26.04.2021 . . . . .	28

## Blog-Serie in drei Teilen

Die Corona Warning App will helfen, sich wieder frei im öffentlichen Raum zu bewegen. Gleichzeitig ist diese Technologie die Büchse der Pandora, bietet Sie eine bislang noch nie dagewesenen Möglichkeit der staatlichen Überwachung. Der CCC bezeichnet diese in seinen 10 Prüfsteinen nicht ohne Grund als Risikotechnologie<sup>1</sup>.

Die ersten Ergebnisse der isländischen App, die von 38% der Bevölkerung genutzt und daher bislang als erfolgreichste App gehandelt wird, sind ernüchternd. Verantwortliche berichten, diese sei keine Hilfe oder gar ein Gamechanger<sup>2</sup>.

Auch die erste Auswertung der RKI Datenspende-App scheint einem netzpolitik.org Beitrag nach ernüchternd zu sein<sup>3</sup>. Die veröffentlichten Karten und Ergebnisse lassen Zweifel an der Sinnhaftigkeit aufkommen, zumal die Auftraggeber keine Ahnung von der zweifelhaften Arbeitsweise der App gehabt hatten und mit Fehlinformationen viel Vertrauen zerstört haben<sup>4</sup>.

Ein Blick in andere Länder, zum Beispiel nach Argentinien, offenbart Datenschutz-Alpträume und offenkundigen Dilettantismus<sup>5</sup>.

Wo stehen wir mit der Corona-Warning-App? Wohin weisen die heute bekannten Informationen? Dieser mehrteilige Beitrag möchte eine Momentaufnahme und Einschätzung geben. Weitere Teile werden in den kommenden Tagen folgen.

### **Vorab aber ein Disclaimer:**

**Im Grunde versuche ich ein sich schnell bewegendes Ziel zu treffen. Bereits Geschriebenes muß bei Erscheinen einer neuen Dokumentation neu überarbeitet werden. Zuvor nicht berücksichtigte Aspekte neu bedacht werden. Ich kann nur „auf Sicht“ schreiben, was nach aktueller Quellenlage als gesichert gilt. Und ich bin als IT-affiner Mensch natürlich nicht ganz Unvoreingenommen und schaue mit einer ganz bestimmten Brille auf die Dinge.**

Wer sich auf eigene Faust einen Überblick in den Repositories der Corona Warning App ver-

---

<sup>1</sup> <https://www.ccc.de/de/updates/2020/contact-tracing-requirements>

<sup>2</sup> <https://www.businessinsider.com/iceland-contact-tracing-not-gamechanger-2020-5>

<sup>3</sup> <https://netzpolitik.org/2020/erste-auswertung-der-datenspende-app-veroeffentlicht/>

<sup>4</sup> <https://www.ccc.de/de/updates/2020/abofalle-datenspende>

<sup>5</sup> <https://nitter.net/mtschirs/status/1261712344561987586>

schaffen und die Entwicklung mitverfolgen möchte, dem empfehle ich dieses am besten ohne Verhaltensdatenweitergabe an Microsoft/GitHub mit einem Mirror zu tun. Wie das datensparsam geht, kann in meinem Blog-Beitrag „Gitea Mirror Spiegel - Die eigene Gitea Instanz Teil III“ gelesen werden.

Warum Telekom und SAP nicht in der Lage sind, ein eigenes VCM zu betreiben, bleibt leider unbeantwortet<sup>6</sup>. Eine eigene GitLab Instanz bietet mindestens genauso gute CI/CD Möglichkeiten.

### **Eine Frage der Prioritäten**

Die Bundesregierung, das RKI als gemeinsame Auftraggeber und die mit der Entwicklung beauftragten Unternehmen Deutsche Telekom und SAP werden im Microsoft/ GitHub Eröffnungsdokument als Stakeholder genannt<sup>7</sup>.

Andere wie zum Beispiel die Gesundheitsämter, die vielen Testeinrichtungen und die Ärzte spielen zwar im Gesamtkonzept eine wichtige Rolle, fehlen aber als Stakeholder. Folglich bleiben Ihre User-Stories und Sichtweisen, die mögliche Anforderungen spezifizieren, unbekannt. Als wenn es da gar keine Anforderungen oder Bedürfnisse zu berücksichtigen gäbe oder diese vollkommen vergessen wurden. Im entsprechenden Issue wird (Nach-)Besserung versprochen<sup>8</sup>.

Ein Datenschutzbeauftragter und eine Datenschutzerklärung sind nicht bekannt. Weder was den Einsatz von Microsoft/ GitHub als zentrale Plattform anbetrifft noch in Form von User-Stories. Eine Projektwebsite existiert nicht, soll aber in Kürze kommen. Wir müssen uns demnach noch gedulden.

Ein Gefahren- oder Threat Modell fehlt bislang ebenso und wird nicht nur von mir vermisst<sup>9</sup>.

Immerhin, für ein App-Logo war hinreichend Muse, Zeit und Geld vorhanden, die Werbeagentur „Zum goldenen Hirschen“ zu beauftragen<sup>10</sup>. Auch Layouts und Farben sollen bereits fest stehen.

---

<sup>6</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/9>

<sup>7</sup> <https://github.com/corona-warn-app/cwa-documentation>

<sup>8</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/69>

<sup>9</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/123>

<sup>10</sup> [https://www.wuv.de/agenturen/zum\\_goldenen\\_hirschen\\_fuehrt\\_corona\\_app\\_ein](https://www.wuv.de/agenturen/zum_goldenen_hirschen_fuehrt_corona_app_ein)

Von Blau und Rot ist die Rede, umrahmt von Claims wie „Kleine App, große Wirkung“, „Die App-traktion des Jahres“ oder auch „Diese App kann nichts, außer Leben retten“<sup>11</sup>.

Wenden wir uns von diesen vorzeitigen, kreativen Ergüssen ab und berücksichtigen den Umstand, dass alles noch „im Werden“ ist.

### **Nun sag, wie hast Du's mit Open Source?**

In einer bemerkenswerten Entscheidung hat die Bundesregierung die Vorgabe gemacht, einen dezentralen Ansatz zu verfolgen und die Quelltexte offen zu legen. Die hier vorgestellten Problemfelder und Inkonsistenzen sollen diese vorbildliche Entscheidung nicht schmälern. Vor einigen Wochen las sich alles noch anders an und liess Schlimmes befürchten<sup>12</sup>.

Diese Transparenz wünschte ich mir gerne auch bei anderen IT Großprojekten, als Stichworte nur Begriffe wie „Anwaltspostfach“, „Herkules“ oder „TollCollect“ in den Raum geworfen. Vielleicht ist es Zeit, so manche Standards für Großprojektmanagement um die Punkte „Open Source“ und „Public Money - Public Code“ als Voraussetzungen in die Köpfe zu bringen.

Bei aller Begeisterung bitte im Hinterkopf behalten, dass die Open Source Corona-Warn-App auf einer mehr oder minder Closed Source Blackbox von Google und Apple aufsetzt, die ihrerseits sich die Hardware mit einer noch größeren Blackbox mit dem Namen Baseband teilt. Die Unterstützung anderer Systeme oder gar eine F-Droid Version wird ausgeschlossen<sup>13</sup>.

Die Gretchenfrage „Nun sag, wie hast Du's mit Open Source?“ entstand zwischen Ankündigung und der ersten Veröffentlichung von Quellcode. Die große Sorge und Frage im Raum war, ob der Quellcode „am Stück“ vor die Füße geworfen wird. Wer zurück an den Mathematikunterricht in der Schulzeit denkt, weiß, wie wichtig nicht nur das Ergebnis sondern auch der Lösungsweg ist. Ich erinnere mich noch sehr gut daran, wie es häufig trotz eines blöden Zahlendrehers am Ende einer seitenlangen Auflösung noch die volle Punktzahl gab. Bei Software verhält es sich ähnlich.

Diese Sorge hat sich nicht bestätigt. Die erste Quellcode-Veröffentlichung ist augenscheinlich vollständig mit Ihren Commits, Branches und Pull Requests. Sogar so vollständig, dass mit

---

<sup>11</sup> <https://www.spiegel.de/netzwelt/apps/corona-bekaempfung-agentur-soll-warn-app-populaer-machen>

<sup>12</sup> <https://www.heise.de/newsticker/meldung/Corona-App-per-PEPP-PT-Kanzleramt-soll-bei-Apple-Druck-machen-4708759.html>

<sup>13</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/5>

einem Schmunzeln gesehen werden kann, wie der cwa-server zuvor ein ena-server war<sup>14</sup>.

Die Gretechenfrage ist beantwortet. Volle Punktzahl trotz Copy & Paste eines Projekt-Templates.

### **Grundannahmen**

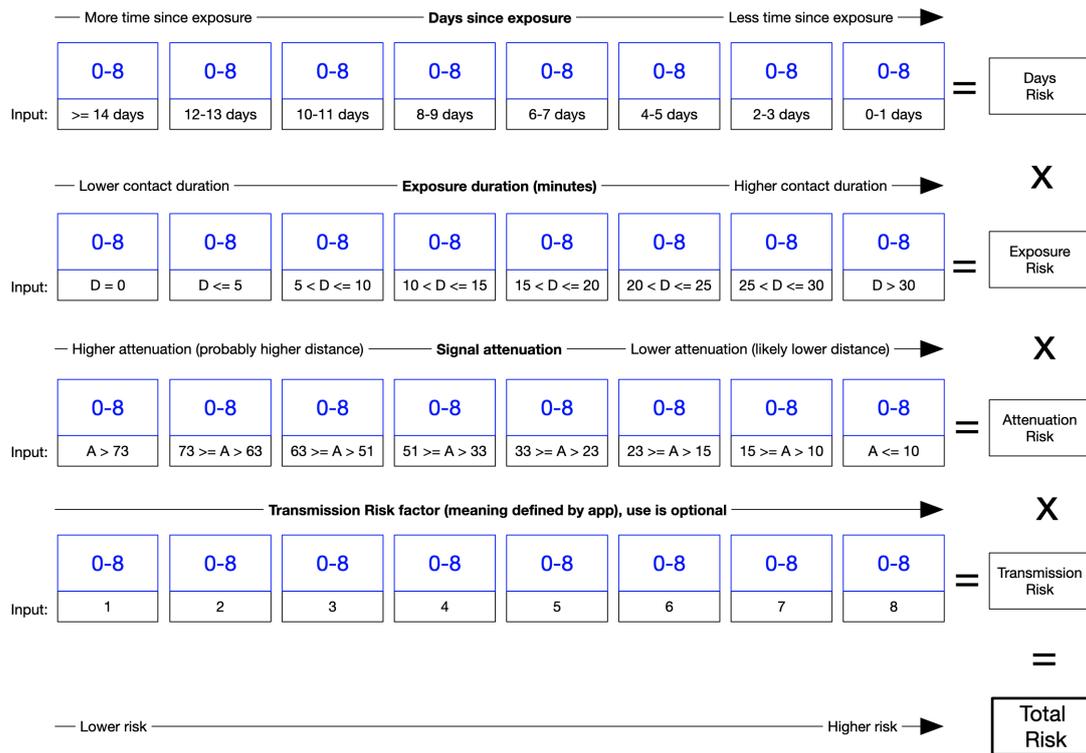
Zur Ermittlung, ob jemand exponiert und möglicherweise erkrankt ist werden folgende Faktoren herangezogen:

- vergangene Tage seit einer Exposition
- Dauer der Exposition (in 5 Minuten Schritten)
- BT Signalstärke
- Mitglied in Risikogruppe (optional)

Mit Ausnahme der optionalen Angabe zur Risikogruppe birgt jeder Faktor so seine Probleme.

---

<sup>14</sup> <https://github.com/corona-warn-app/cwa-server/commit/2bd45ddc36517f1a7e43772ea54acfb0c79563d>



**Abbildung 1:** Faktoren

**Abstandsmessung**

An der Abstandsmessung mit BT LE scheiden sich die Geister<sup>15</sup>. Es handelt sich dabei um keine direkte Messung wo ein Wert X eine Distanz Y ergibt sondern um eine interpretierte Messung, wo zahlreiche Störfaktoren beseitigt und mit Gauss- oder Sigmoid-Funktionen mathematische Schwellenwerte und Stufen erst ermittelt werden müssen.

Obwohl mehrere PEPP-PT Testreihen stattgefunden haben, geben diese alle mehr oder minder Laborumgebungen wieder ohne besondere Berücksichtigung von Hindernissen, Reflektionen oder Interferenzen. Der Aussage eines Issues nach soll das Umarmen einer Person mit beiden Smartphones in der Tasche sich kaum von dem Signalmuster von in der Hand gehaltenen

<sup>15</sup> <https://www.golem.de/news/coronakrise-schneier-haelt-contact-tracing-apps-fuer-unbrauchbar-2005-148227.html>

Geräten im Sicherheitsabstand von 2 Metern unterscheiden<sup>16</sup>.

Die Aufzeichnungen der verlinkten PEPP-PT Testreihe „Distance Measurements and Classification Test Report“ von Dipl-Inf Steffen Meyer, Fraunhofer IIS scheint dieses zu bestätigen<sup>17</sup>.

Auch schreibt dieser:

Estimating proximity by measuring RSS can be influenced by a number of parameters, including phone model (antennas, BLE chip), usage pattern (in hand, at ear, in pocket), environment (indoor/outdoor, open space / crowded rooms), phone orientation and others. However, RSS-based positioning is widely spread and has to cope with the same effects.

In einem deutlich aufwändigeren Test mit mehreren Geräten, 48 Bundeswehrsoldaten, Indoor- und Outdoor-Messungen liefert das Paper „Report from the Measurement Campaign 2020-04-09“ der Forscher Jackie Ma, David Neumann, Felix Sattler, Ralf Schafer, Patrick Wagner, Thomas Wiegand bessere Resultate<sup>18</sup>.

Based on the values (..) the actual distances (ground truth) of all the mobile phones involved in the test can be determined.

Im gleichen Paper steht in einem Nebensatz vermutlich der beste Hinweis, was die App wirklich messen soll:

(...) according to the Robert Koch Institute, for the flu, a physical proximity between two people of less than 2 meters over a time period of 900 seconds (15minutes), results in a high risk of being infected.

Im Paper wird eine Erkennungsrate (True Positive Rate) zwischen 67% und 76% detektiert.

Den ersten Prüfstein<sup>19</sup> des CCC als Maß angesetzt:

---

<sup>16</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/85>

<sup>17</sup> <https://github.com/pepp-pt/pepp-pt-documentation/blob/master/12-proximity-measurement/distance-measurements-and-classification-20200406.pdf>

<sup>18</sup> <https://github.com/pepp-pt/pepp-pt-documentation/blob/master/12-proximity-measurement/2020-04-09-BW-report-epi-mod.pdf>

<sup>19</sup> <https://www.ccc.de/de/updates/2020/contact-tracing-requirements>



Statistisch betrachtet: Wenn die App wirklich nur alle 5 Minuten für 2 Sekunden lauscht, ergibt das über einen Tag mit 24 Stunden und 86.400 Sekunden ein Zeitfenster von 576 Sekunden oder 0,67% der Zeit.

Der technischen Einschränkungen ist man sich bei den Stakeholdern bewusst:

(...) only exposures of longer duration within a certain proximity range are considered relevant for the intended purpose of this app, most of them will be covered.

Passen die grundlegenden Annahmen? Was ist von einem Instrument zu halten, das nur 0,67% der verfügbaren Zeit misst? Einerseits bin ich als IT-Mensch von der Möglichkeit fasziniert, wie mit minimalinvasiven 0,67% der Zeit alle Kontakte und Interaktionen > 5 Minuten abbildbar werden. Andererseits aus einer datenschutzrechtlichen Sicht bin ich tief erschüttert.

### **Differenzen und Unsicherheiten**

Wo die Grundannahmen zwischen den Stakeholdern zu 100% auseinander klaffen wird in der Bandbreitenberechnung deutlich. Das RKI geht von einem „best case“ von 60 Mio Anwendern aus, SAP und Telekom von 30 Mio<sup>21</sup>.

Darüber hinaus will das RKI sich die Möglichkeit offen halten, die Gewichtung der einzelnen Faktoren mit einem zusätzlichen „Weight Factor“ justieren zu können. Dieses soll vorbei an den App-Stores zusammen mit der Übermittlung von Diagnosedaten erfolgen. Wie genau ist noch nicht bekannt<sup>22</sup>.

### **Aufbau der Gesamtlösung**

Betrachten wir die angedachte Funktionsweise der Gesamtlösung, bestehend aus den nativen iOS- und Android-Apps sowie den Serverdiensten. Der Onboarding-Prozess, wie eine App sich auf einem Gerät initialisiert und wie die anonyme Übermittlung von Diagnosedaten Infizierter ausgestaltet ist, lässt sich noch nicht sagen.

---

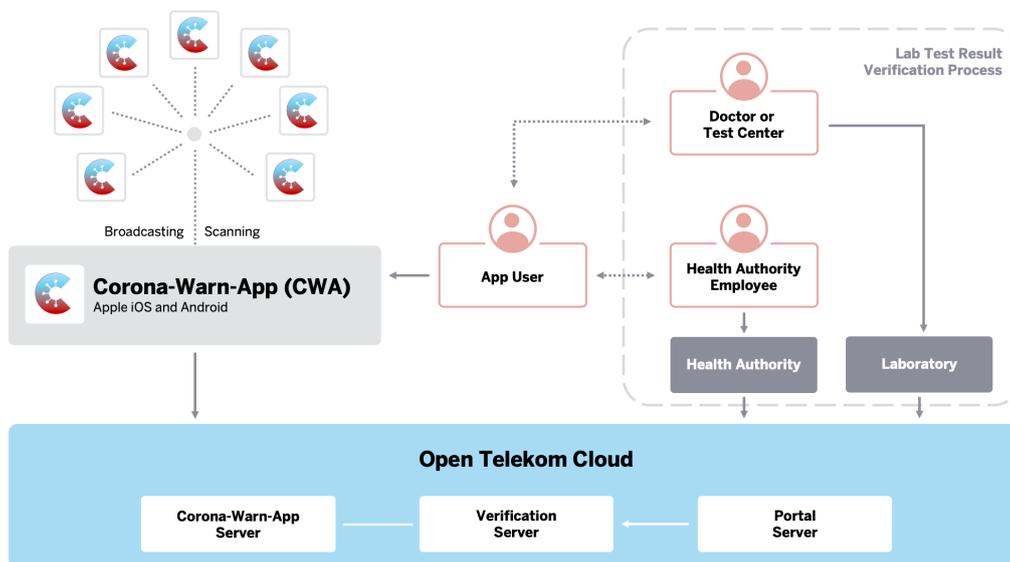
<sup>21</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/95>

<sup>22</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping\\_document.md#parameter-settings](https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping_document.md#parameter-settings)

Was sich bereits jetzt sagen lässt ist, dass keine Push Notification Services von Google und Apple zum Einsatz kommen werden. Diese könnten Hinweise und zusätzliche Mißbrauchsmöglichkeiten für Dritte bieten, dazu später mehr im letzten Teil der Blog-Serie.

Kommuniziert wird direkt mit den Servern der Telekom, die in der Open Telekom Cloud (OTC) betrieben werden. Damit die App das auch sicher kann, spendieren Apple und Google systemseitig mehr „background time“<sup>23</sup>.

Wir dürfen uns auf einen erhöhten Strombedarf und somit deutlich kürzere Laufzeit von teilnehmenden Endgeräten einstellen. Immerhin nirgends steht etwas von Cloudflare oder US-CDNs, das ist soweit gut.



**Abbildung 3:** Aufbau

Die bereits bekannte Zahl aus der „Bandwidth Estimation“ geht von ca. 30 Mio Anwendern aus, die ein Datenvolumen von 43 TB und 720 Mio Requests am Tag erzeugen sollen<sup>24</sup>.

Gemäß dieser Zahlen leitet sich ab, dass die App vermutlich einmal stündlich Kontakt mit Ihren

<sup>23</sup> [https://developer.apple.com/documentation/exposurenotification/building\\_an\\_app\\_to\\_notify\\_users\\_of\\_covid-19\\_exposure](https://developer.apple.com/documentation/exposurenotification/building_an_app_to_notify_users_of_covid-19_exposure)

<sup>24</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/master/solution\\_architecture.md#bandwidth-estimations](https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md#bandwidth-estimations)

Gegenstellen aufnimmt. Ausgehend von 2.000 täglichen Neuinfektionen wird der Umfang der übermittelten Diagnosedaten auf ca. 1,5 MB geschätzt. Das ergibt für jedes Endgerät:

- 36 MB/ Tag
- 252 MB/ Woche
- ca. 1 GB/ Monat

Ich befürchte das Thema Netzneutralität wird in der einen oder anderen Form wieder auf den Tisch kommen. Hat doch ausgerechnet die Telekom in der Vergangenheit mit Ihren StreamOn- und Zero-Rating Produkten eine nicht als legal zu bezeichnende Auffassung vertreten<sup>25</sup>.

---

<sup>25</sup> <https://www.heise.de/newsticker/meldung/Netzneutralitaet-Telekom-muss-StreamOn-aendern-4470789.html>

## Teil II - in the meantime

Wurde ich während des Schreibens vom ersten Teil von einer neuen Dokumentation und dem ersten Quellcode überrascht, so war das beim zweiten Teil die neue Projektwebsite und die Fertigstellung der Apple/Google API mit dem Namen „Exposure Notification“. Diese wird bereits aktiv via iOS 13.5 Update bzw. Android-Playstore verteilt<sup>26</sup>.

Wer die Links zu den Dokumentationen haben möchte:

- Android-Dokumentation
- iOS-Dokumentation

Unterstützt werden alle Android ab Version 6 mit BTLE Hardware. Bei Apple ist BTLE kein Faktor und seit dem iPhone4 in allen Geräten enthalten. Der 2 GB RAM-Bedarf des iOS 13 Betriebssystems ist da der limitierende Faktor. Über diesen verfügen erst die Geräte ab dem iPhone 6S. Vereinfacht gesagt werden alle Geräte unterstützt, die nicht älter als 4-5 Jahre sind<sup>27</sup>.

Werfen wir einen Blick in die Statistik:

- ca. 75% aller Androiden wird unterstützt<sup>28</sup>.
- Es existieren 58 Mio Smartphones in Deutschland<sup>29</sup>.
- Das Verhältnis Android zu iOS Geräten liegt bei ca. 4:1<sup>30</sup>.

Über's Knie gerechnet ergibt das einen „best-case“ von 43 Mio Geräten (34 Mio Android, 9 Mio iOS). Das ist knapp die Hälfte der Gesamtbevölkerung von 83 Mio. Auf der anderen Seite haben wir den „worst-case“ mit 0,5 Mio für die RKI Datenspende App<sup>31</sup>.

---

<sup>26</sup> <https://www.heise.de/news/iOS-13-5-Apple-bringt-Corona-Update-4726116.html>

<sup>27</sup> [https://en.wikipedia.org/wiki/IOS\\_13#Supported\\_devices](https://en.wikipedia.org/wiki/IOS_13#Supported_devices)

<sup>28</sup> <https://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os>

<sup>29</sup> <https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenuutzer-in-deutschland-seit-2010>

<sup>30</sup> <https://de.statista.com/statistik/daten/studie/256790/umfrage/marktanteile-von-android-und-ios-am-smartphone-absatz-in-deutschland>

<sup>31</sup> <https://netzpolitik.org/2020/erste-auswertung-der-datenspende-app-veroeffentlicht>

Die goldene Mitte läge demnach bei 22 Mio. Persönlich tendiere ich eher auf 10-15 Mio. Jemand möge mich bitte im Dezember an diese Zahlen erinnern.

Zur neuen Website ist zu sagen, dass diese zwar um Datenschutz bemüht ist. Im Detail fehlten dann doch wichtige Security- und Privacy-Features. Als schwerwiegend erachte ich TLS 1.0, die fehlende CSP und die offenkundig nicht definierte Abstimmung zwischen den Teams<sup>32</sup>.

Eine 404 „Seite nicht gefunden“ ist noch schön gestaltet. Bis zu einem 405 „Methode nicht erlaubt“ (oder anderen HTTP Fehlercodes) reichte die Kreativität der goldenen Hirsche offensichtlich nicht mehr<sup>33</sup>.

Bevor es weitergeht möchte ich aber eines positiv hervorheben: Wie die Jungs von SAP auf Fragen eingehen und Einblick auch in laufende interne Diskussion geben ist vorbildlich und professionell. Dass ich von „Jungs“ rede ist nicht diskriminierend. Im sechs-köpfigen Entwicklungs- und Dokumentationsteam gibt es zum Zeitpunkt des Schreibens dieses Blogs keine Frau<sup>34</sup>.

### **Fortsetzung: Aufbau der Gesamtlösung**

Das Server-Backend, die Gegenstelle der mobilen Apps basiert auf einer Open Shift Container-Plattform bestehend aus skalierbaren Docker-Containern. Die App wird dabei mit drei Gegenstellen kommunizieren<sup>35</sup>:

- Verification Server
- CWA-Server
- Portalserver

Eine genaue Abgrenzung zwischen CWA-Server und Portalserver wird mir noch nicht ersichtlich. Grob betrachtet soll der Portalserver den Transfer der Daten übernehmen, während der CWA-Server eher die Steuerzentrale in der Kommunikation und Freigabe von Testresultate und Diagnosedaten ist.

---

<sup>32</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/137>

<sup>33</sup> Bild Fehlermeldung

<sup>34</sup> <https://github.com/orgs/corona-warn-app/people>

<sup>35</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/master/images/solution\\_architecture/CWA\\_Components.png](https://github.com/corona-warn-app/cwa-documentation/blob/master/images/solution_architecture/CWA_Components.png)

Die Kommunikation unter den Servern erfolgt über TLS gesicherte JSON-Webservices<sup>36</sup>. Die Webservices sind in JAVA/Maven programmiert mit einem ganzen Zoo an Toolchain wie JaCoCo oder sonarcloud, das einem im sonarcloud Dashboard eine bessere Code-Analyse verschafft.

Was die Hochverfügbarkeit betrifft liegt die Projekt-Website hinter mehreren Endpoints. Ich konnte die IPs 87.148.208.250, 87.140.209.25-27 identifizieren. Gut möglich, dass hier auch die späteren Container für die Webservices laufen.

Wirklich viel an Code gibt es nicht zu sehen, da bislang nur das Grundgerüst steht und die Arbeit erst nach Veröffentlichung des Apple/Google Frameworks beginnen kann. Um ein Code-Beispiel zu zeigen: Die Überprüfung von TANs und teleTANs sieht noch so aus:

```
1  private boolean validateTan(String tan) {
2      // FIXME Add implementation
3      return true;
4  }
5
6  private boolean validateTeleTan(String teleTan) {
7      // FIXME Add implementation
8      return true;
9  }
```

Auf der Datenbankseite existieren so weit ersichtlich zwei Systeme:

- zenko.io Object Storage
- Postgres

Der verwendete Postgres Server liegt zwar in einer aktiv betreuten Version 9.6 vor<sup>37</sup> ist aber dahingehend als unglücklich zu betrachten da diese Version nächstes Jahr End-Of-Life sein wird und keinen Support erhält. Warum auf eine ältere Version zurück gegriffen wird ist schwer zu sagen. Es ist vorstellbar, dass es in der Toolchain etwas gibt, was das vorgibt. Die aktuelle Postgres-Version ist 12.3<sup>38</sup>.

Hinsichtlich dem Object-Storage ist zu betonen, dass in den Dokumenten häufig die Rede von „S3“ ist. Das bedeutet nicht, dass dieser bei Amazon liegt. Zenko ist eine Open Source Plattform, die eben genau einen Vendor Lock-In verhindern soll. Gehostet wird alles bei der

---

<sup>36</sup> <https://github.com/corona-warn-app/cwa-server/blob/master/docs/images/v4.png>

<sup>37</sup> <https://github.com/corona-warn-app/cwa-server/issues/180>

<sup>38</sup> <https://www.postgresql.org/support/versioning/>

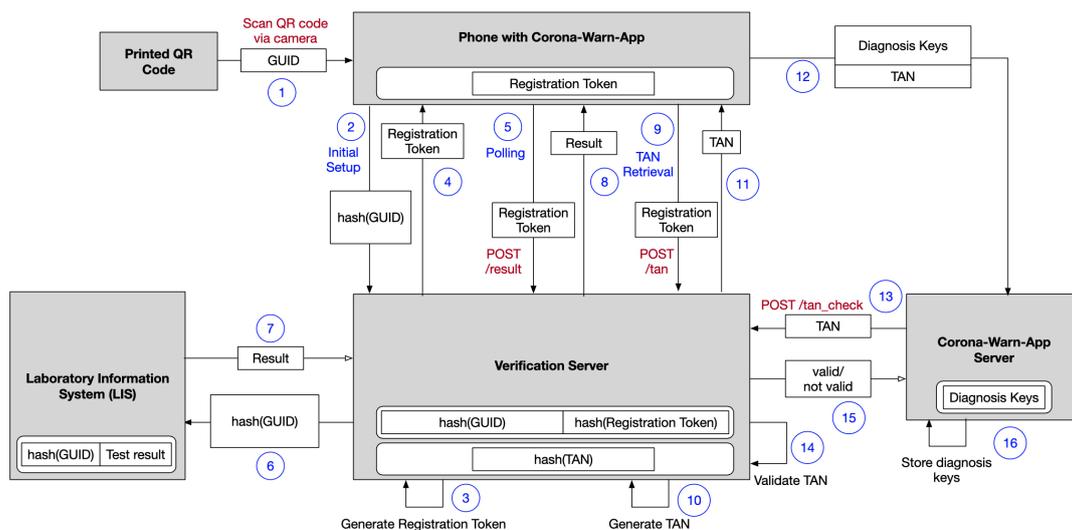
Telekom, das wurde mir auf Nachfrage extra bestätigt<sup>39</sup>.

Was mir die Tage aber in den Kopf kam, war der Skandal um die bei Amazon liegenden Videos der Bundespolizei. Für nur 2.000 Body-Cams mit einem Bruchteil an Datenvolumen einer Corona-App, gäbe es angeblich keine heimische Alternative<sup>40</sup>.

Eine Schnittstelle besteht zum zentralen Laborsystem der Testeinrichtungen sowie zu den Mitarbeitern der Gesundheitsämter, wo teleTANs für den manuellen Datenabgleich erstellt werden. In welcher Form ist noch unklar.

## Der Schlüsselmeister in der Matrix

Zentrales Element in der Infrastruktur bildet der Verification Server. Über diesen erfolgen sämtliche Authentifizierung und vor allem der Akt der De-Anonymisierung eines Geräts bei der Übermittlung von Testergebnissen, sofern dieses nicht zuvor mit Abgleich zu andern Datentöpfen erfolgt ist, dazu später mehr. Der Ablauf - soweit einsehbar und verstanden - sieht wie folgt aus:



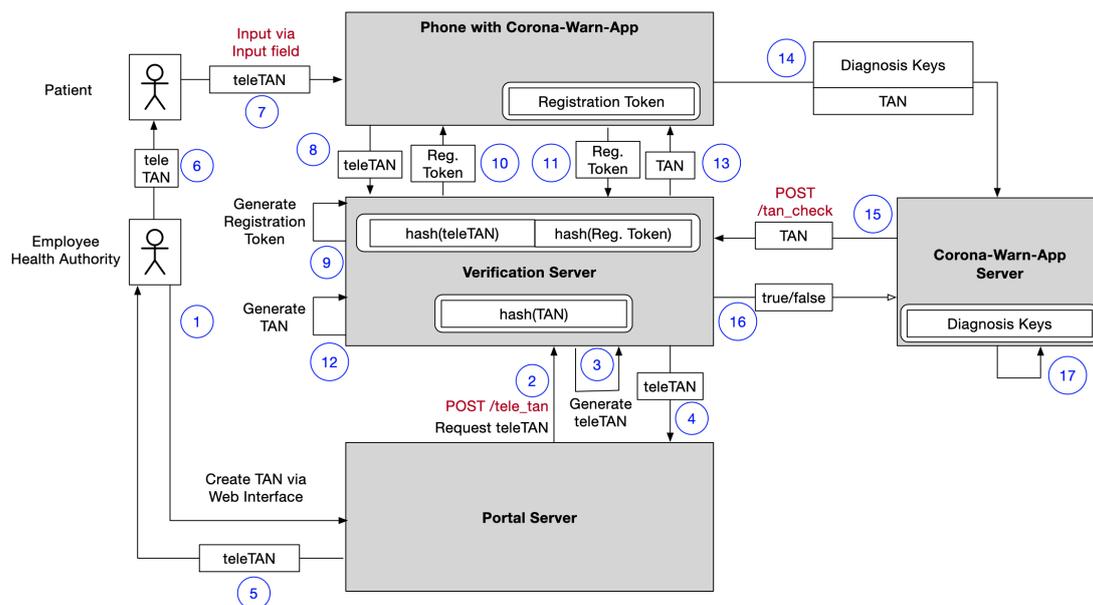
**Abbildung 4:** Ablauf

<sup>39</sup> <https://github.com/corona-warn-app/cwa-server/issues/234>

<sup>40</sup> <https://netzpolitik.org/2019/bundespolizei-speichert-bodycam-aufnahmen-weiter-bei-amazon>

Soweit verstanden, erstellt die App einen gerätebezogene GUID-Hash. Ein Hinweis in der Cross-Border-Interoperability macht deutlich, dass man sich hier wohl auf die API der Hersteller verlässt<sup>41</sup>.

Die GUID wird als Hash an den Verification Server gesendet und daraus ein Registration Token abgeleitet. Anschliessend wird dieser wieder zurück an den Clienten gesendet. Am Server verbleiben nur die Hashes. Ob noch weitere Bestandteile oder Salts zum Einsatz kommen bleibt wie das übrige kryptografischen Verfahren noch unklar.



**Abbildung 5:** Ablauf mit teleTANs

Was fest steht ist, dass es in Folge zu einem Ping-Pong zwischen Smartphone mit TANs, teleTANs und der Übermittlung der Diagnosedaten kommen soll aufgrund der Anforderung, neben dem direkten Weg auch einen manuellen, händischen anzubieten. Die Kommunikation erfasst auch die Zusendung der GUID Hashes an die Systeme der Labore, die damit die Testergebnisse verschlüsseln<sup>42</sup>.

<sup>41</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/master/solution\\_architecture.md#cross-border-interoperability](https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md#cross-border-interoperability)

<sup>42</sup> [https://raw.githubusercontent.com/corona-warn-app/cwa-documentation/master/images/solution\\_architecture/figure\\_3.svg](https://raw.githubusercontent.com/corona-warn-app/cwa-documentation/master/images/solution_architecture/figure_3.svg)

Die Komplexität wird zusätzlich erhöht indem JSON-Aufrufe von /result und /tan zur Übermittlung der Testergebnisse mit Zufallsdaten, sogenannten „Dummy Submissions“ verschleiert werden sollen<sup>43</sup>.

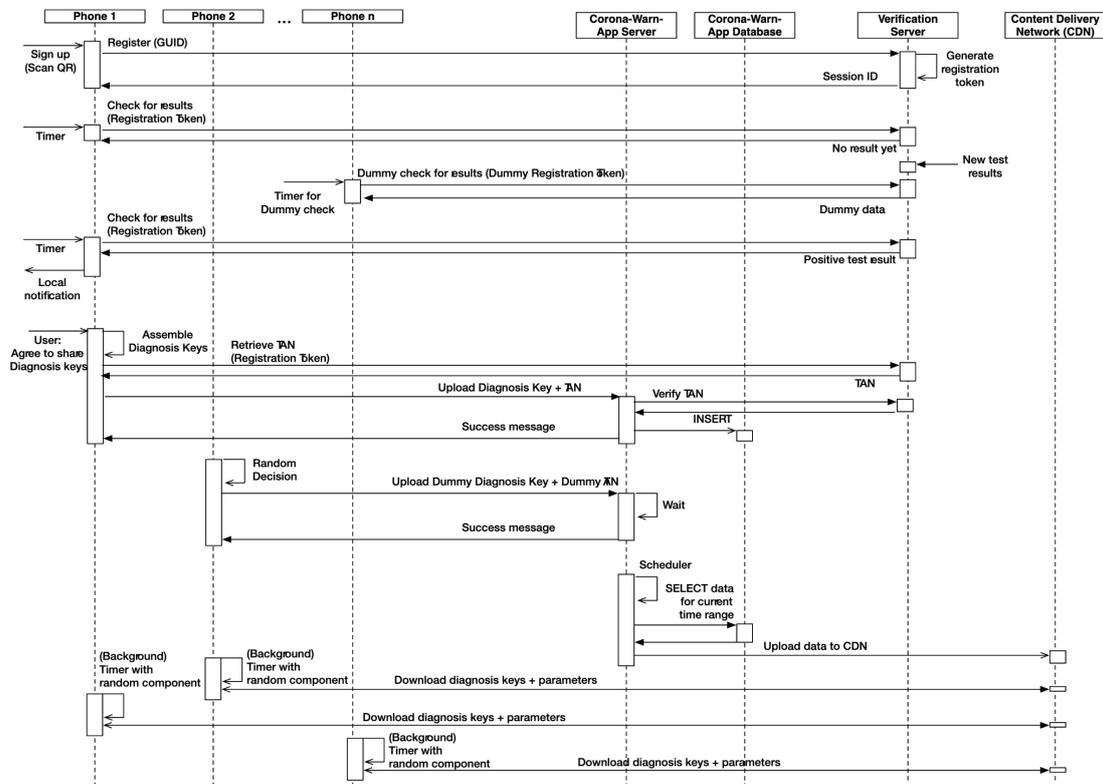


Figure 7: Interaction of the mobile application(s) with the backend servers and CDN

**Abbildung 6: Kommunikation**

**Komplexität**

Gleich auf mehreren Wegen soll es einem Benutzer ermöglicht werden, Testergebnisse mit der App zu erhalten bzw. Diagnosedaten zu übermitteln. Alles zusammengefasst in nachfolgenden User-Stories<sup>44</sup>

<sup>43</sup> [https://raw.githubusercontent.com/corona-warn-app/cwa-documentation/master/images/solution\\_architecture/figure\\_7.svg](https://raw.githubusercontent.com/corona-warn-app/cwa-documentation/master/images/solution_architecture/figure_7.svg)

<sup>44</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping\\_document.md](https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping_document.md)

As a user of the app, I want to be able to scan a QR code provided by my doctor or test center, so that I can receive my test result in the Corona-Warn-App.

As a user of the app, I want to be able to use a manual process (in addition to the digital process), for example, through a call center and without a QR code, to send the pseudonymized IDs, under which I was visible to other app users in recent days, to the Warn server so the people I have been in contact with can be warned by their apps.

As an app user, I want to be able to enter a TAN in the app, to use the TAN I have been given to assign my test result to my instance of the app.

Neben einem digitalen Weg mit QR-Code soll es einen zweiten, manuellen Weg mit einer teleTAN geben. Diese teleTAN soll „human readable“ sein, was auf eine Zahlen- oder Buchstabenkombination mit geringer Entropie hindeutet<sup>45</sup>.

Im „Scoping Document“ unter dem Punkt User-Story E06.04 ist von Callcentern die Rede, die eine teleTAN aushändigen sollten<sup>46</sup>.

Im „Solution Architecture“ Dokument hingegen ist die Rede von „health authority“, also von Mitarbeitern eines Gesundheitsamtes<sup>47</sup>.

Wissen die von Ihrem Glück? Noch ist nichts von einer Authorisierung oder Authentifizierung von Mitarbeiter zu lesen. Was jedoch bekannt ist, daß diese als Stakeholder bislang nicht einbezogen waren und daß mancherorts Gesundheitsämter an Ihrer Belastungsgrenze arbeiten und unterbesetzt sind<sup>48</sup>.

Was, wenn am Ende doch ein namenloser Call-Center-Agent über die Verteilung von teleTAN bestimmt? Technisch kann nicht verhindert werden, dass jemand die App auf mehreren Geräten

---

<sup>45</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/5743969ddbef953c2aa40aeac3122ab533540411/solution\\_architecture.md#retrieval-of-lab-results-and-verification-process](https://github.com/corona-warn-app/cwa-documentation/blob/5743969ddbef953c2aa40aeac3122ab533540411/solution_architecture.md#retrieval-of-lab-results-and-verification-process)

<sup>46</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/e41b87fc9ae81fa85e5243abc722d12b6308648b/scoping\\_document.md](https://github.com/corona-warn-app/cwa-documentation/blob/e41b87fc9ae81fa85e5243abc722d12b6308648b/scoping_document.md)

<sup>47</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/e41b87fc9ae81fa85e5243abc722d12b6308648b/solution\\_architecture.md](https://github.com/corona-warn-app/cwa-documentation/blob/e41b87fc9ae81fa85e5243abc722d12b6308648b/solution_architecture.md)

<sup>48</sup> <https://www.ndr.de/nachrichten/info/Zu-wenig-Personal-in-vielen-Gesundheitsaemtern,gesundheitsaemter100.html>

nutzt. Es kann auch nicht ausgeschlossen werden, dass ein Berechtigter eine teleTAN anfordert und an einen anderen weitergibt<sup>49</sup>.

### **Komfortfunktionen vs. Corona**

Am meisten erstaunen die vielen „Komfortfunktionen“ im „Scoping Document“. Das sind beispielsweise allgemeine Informationen, was bei einer Infektion zu tun sei (User-Story E05.02). Dabei sollen die Inhalte dynamisch anpassbar und vom RKI zentral in einem Content-Management-System (User-Story E10.01) gepflegt werden<sup>50</sup>.

Wie ist ein Verhalten zu interpretieren, wo kurz nach einem Datenabgleich plötzlich angefangen wird Erklärvideos oder Informationstexte im Internet zu öffnen? Auch wenn niemand sieht, was abgerufen wird, ermöglichen Metadaten wie z.B. Dauer, Datei- und Verzeichnisnamen gewisse Rückschlüsse.

Ich persönlich halte es für unverständlich, warum in Anbetracht der kurzen und holprigen Entwicklungszeit die Komplexität mit solchen Anforderungen erhöht wird. Reichen die bestehenden Informationsangebote nicht aus? Müssen diese diese wirklich auch noch in die App integriert werden? Jedes zusätzlichen Feature - zumal auch noch remote durch ein Content Management System verwaltet - reduziert die Anonymität und die Dezentralität<sup>51</sup>.

---

<sup>49</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/41>

<sup>50</sup> [https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping\\_document.md](https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping_document.md)

<sup>51</sup> <https://github.com/corona-warn-app/cwa-documentation/issues/13>

## Teil III - in the meantime

Seit dem zweiten Teil ist einiges passiert. Erste Versionen der Android- und iOS-Apps sind erschienen, die Repositories der Server-Backends und auch die Website<sup>52</sup>.

Ich kann es gar nicht so oft und deutlich hervorheben: Was das Projektteam - zwischenzeitlich ist auch ein Mädels hinzugekommen - hier macht ist für ein derart medienwirksames Public-Private-Projekt in Deutschland bislang einmalig, die Vorgehensweise mustergültig. Wenn Vorschläge, Fragen, selbst die eine oder andere qualifizierte Kritik über den dafür vorgesehenen Kanal Github kommen, dann ist das für eine Open Source Software als normal zu bezeichnen.

Es geht weiter mit dem letzten Teil meiner kurzen Serie. Viel Spaß beim Lesen!

### App ist nur ein Baustein

Die Corona-Warning-App ist nur ein Baustein von mehreren. Wie im letzten Teil gesehen sind die Serverdienste und Schnittstellen im Backend, die Infrastruktur dahinter wichtiger. Sicherheitstechnisch spielt dort die Musik. Dort melden sich Mitarbeiter von Callcentern und Gesundheitsamt an, dort besteht eine Kommunikation über Schnittstellen zu anderen Systemen (zu einem davon gleich noch ein paar Worte).

Positiv zu erwähnen ist, dass eine OpenID und 2-Faktor Authentifizierung in der Dokumentation vorgesehen sind. Client-Zertifikate sichern ihrerseits die Server-zu-Server Kommunikation ab<sup>53</sup>.

Daher lehne ich mich aufgrund der Feststellungen und Beobachtungen in den ersten beiden Blogteilen beruhigt aus dem Fenster und behaupte, dass die App auf den Geräten unkritisch sein wird. Von vielleicht kleineren Fehlern abgesehen, passen Methodik und die eingesetzten Tools. Es wird offen und nativ für die jeweiligen Systemen programmiert und ich erwarte keine groben handwerklichen Schnitzer.

Was der ganzen Architektur jedoch fehlt ist der Nachweis, dass die Version auf den Servern auch den aus den Repos entspricht. Wer auditiert und garantiert einem, dass keine „Erweiterungen“ installiert wurden? Diese Lücke ist kaum nachprüfbar.

---

<sup>52</sup> <https://github.com/corona-warn-app>

<sup>53</sup> <https://github.com/corona-warn-app/cwa-verification-portal/blob/master/docs/architecture-overview.md>

## **Abnormale User-Stories**

Kommen wir zu den abnormalen Dingen. Eine Gruppe von Aktivisten und Wissenschaftlern hat im Rahmen der P3P zahlreiche Beispiele gesammelt und auf Ihrer Website zusammengeführt<sup>54</sup>.

Beim Lesen wird offenbar, wie verwundbar wir trotz maximaler Sicherheit und Datenschutz bleiben. Alle nachfolgenden Beispiele kommen ohne Hacking der Geräte oder der Kommunikation aus und decken Schwächen „by Design“:

### **Ist jemand krank?**

Jemand möchte wissen, ob und wann seine Mitbewohner erkranken. Dafür reicht ein altes Zweitgerät mit installierter App, das im Treppenhaus oder hinter dem Eingangsbereich als statischer Empfänger für eine gewisse Dauer alle RPI einsammelt. Meldet sich ein Nachbar als infiziert, erfährt es zeitgleich auch ein Dritter. Es mag unkritisch klingen doch wie verhält es sich bei einem Paparazzo, einem Stalker, Vermieter oder Arbeitgeber?

### **Bewerbungsgespräch**

Eine wichtige Stelle für ein zeitkritisches Projekt wird vergeben. Drei gleich gute Bewerber stellen sich vor. Für jeden wird jeweils ein extra Smartphone mit der App während des Vorstellungsgesprächs positioniert. Nach 14 Tagen erfolgt die Entscheidung, wen man nimmt und wen nicht. Ein Blick auf die drei Geräte zeigt dem Arbeitgeber an, wer für die nächste Zeit besser nicht genommen werden sollte.

### **Die Verhinderung**

Ein Fußballspieler ist wichtiger Akteur in einem anstehenden Champions-League Spiel. Um zu verhindern, dass dieser spielt, reicht es aus, sein eigenes Mobiltelefon in die Nähe zu bringen und sich anschliessend krank zu melden. Oder einem Erkrankten aber noch nicht gemeldeten sein Handy weiterzugeben. Der Spieler erhält eine Benachrichtigung und muss sich in Quarantäne begeben.

---

<sup>54</sup> <https://tracing-risks.com/>

### **Der Systemgegner**

Ein Systemgegner zeigt erste Symptome von COVID-19. Um möglichst großen Schaden anzurichten, befestigt er sein Smartphone am Halsband seines Hundes und lässt diesen beim Spaziergang frei herumlaufen. Oder er lässt eine Drohne mit dem Smartphone im Gepäck über die Häuser anderer hinreichend lange - in den Dokumenten ist von 10-15 Minuten Expositions-Dauer die Rede - schweben oder er wandert absichtlich an möglichst viele Orten, bevor er sich testen lässt. Solche Menschen könnten demächst im Darknet besonders gesucht werden und sich über zusätzliche Einnahmemöglichkeiten freuen.

### **Der Bart-Simpson-Typ**

Eine Klausur steht an, die ein Schüler oder Student nicht schreiben will. Im Darknet erfährt er die gehandelten Kontaktdaten eines anderen Infizierten mit Symptomen, der noch nicht offiziell getestet wurde. Man vereinbart, die Telefone zu tauschen. Mit dem neuen Gerät geht der Schüler überall in seiner Schule umher. Wird der bislang ungetestete Fall (des Infizierten) offiziell, erhalten alle Mitschüler und Lehrer die Benachrichtigung, in Quarantäne zu gehen.

Bei einigen der gezeigten Beispielen wird der Einwand kommen, niemand habe die Absicht, eine Überwachungs-Infrastruktur aufzubauen. Niemand wird gezwungen, eine solche App zu laden. Benachrichtigungen können auch ignoriert werden, Testergebnisse auf den bekannten manuellen Wegen verarbeitet werden. Ist das glaubhaft wenn gleichzeitig mit „Komfortfunktionen“ Nudging betrieben wird? Politiker wie ein gewisser Axel Voss preschen bereits hervor und möchten Restaurantbesuche und Reisen von der App-Nutzung abhängig machen<sup>55</sup>?

### **Function Creeping**

Mit diesem Begriff sind Maßnahmen gemeint, die vermeintlich planlos immer wieder etwas „dranflanschen“. Dabei erscheint jeder kleine Schritt, jede neue Funktion, allein betrachtet nicht schlimm. Wer bei einem kleinen Update, oder einer Optimierung gleich mit einer Grundsatz-Diskussion beginnt, riskiert sogar schräg angeschaut zu werden. Die viele kleine Trippelschritte bergauf enden irgendwann auf dem Berggipfel.

---

<sup>55</sup> <https://www.faz.net/aktuell/politik/wer-die-corona-app-hat-soll-zuerst-wieder-ins-restaurant-duerfen-16759932.html>

Eine aus guten Gründen eingeführte App, kann sich im Nachhinein als eine Büchse der Pandora erweisen. Gute Gründe sind immer relativ und können sich jederzeit ändern. Was passiert, wenn künftige Interpretationen heutiger Begriffe sich Bahn brechen? Heute ist es COVID-19, morgen vielleicht Sinti und Roma? Jemand möge sich einmal bitte die Aussagen des US-Bundesstaates Minnesota auf der Zunge zergehen lassen, aufgrund der aktuellen Unruhen in den USA die dortige Contact-Tracing App zur Verfolgung von Black-Lives-Matter Demonstranten einzusetzen<sup>56</sup>.

Wir brauchen aber gar nicht so weit zu gehen. Erinnern wir uns an das offenkundig krude Rechts- und Technikverständnis des BND. Bei der Frage, was denn eine „Maschine-Maschine“ Kommunikation sei antwortete ein hochrangiger Beamte, dass dieses aus Sicht des BND das Einbuchten eines Smartphones an einen Funkmast sei. Sämtliche rechtliche oder datenschutzrechtliche Rahmen würden somit entfallen, da diese nur bei einer Kommunikation zwischen Menschen gelten würde<sup>57</sup>.

### **Daten vs. Selbstbelastungsfreiheit**

Es ist eine Errungenschaft unseres Rechtsstaats, dass sich ein Beschuldigter nicht selbst belasten muß. Selbst die Pflichtangaben zur Person wie Name, Adresse, Beruf, Nationalität etc. können mitunter verweigert oder intelligenter: Mit Pseudo- und Fake-Angaben beantwortet werden, da bereits mit Kenntnis dieser Daten mit einer gewissen Präjudiz einhergehen könnte. Einen schönen Blog dazu hat unlängst der Anwalt Hoenig aus Berlin geschrieben<sup>58</sup>.

Die Selbstbelastungsfreiheit wird zur Farce, wenn wir unsere Daten nicht im Griff halten und einst freigegebene Daten nicht zurückrufen oder gar löschen können.

Jetzt mag jemand einwenden „ich bin kein Krimineller“ oder es kommt der allseits bekannte Spruch „Ich habe nichts zu verbergen“. Eine sehr einfache Sicht der Dinge. Was passiert, wenn jemand zu Unrecht etwas bezichtigt wird? Wenn die heutige Frau oder Freundin sich morgen trennt und einem aus verfahrenstaktischen Gründen für die besseren „Argumente“ unterschiebt? Bei einer Umgangs- und Sorgerechtsregelung der gemeinsamen Kinder zum Beispiel?

---

<sup>56</sup> <https://nitter.net/NBCNews/status/1266758240018276352>

<sup>57</sup> <https://logbuch-netzpolitik.de/lnp346-grundrechtsimperialismus>

<sup>58</sup> <https://www.hoenig.de/2020/angaben-zur-selbstbelastung/>

## Was ist ein Leben wert?

Diese Frage sollte jeder mit sich selbst ausmachen. Grundsätzlich trackt jedes Android-Gerät umfassender und sogar mit genauen GPS-Positionen seine Benutzer als es die Corona-Warning-App könnte. Die norwegische Behörde für Konsumschutz zeigt das in Ihrem kurzen Video sehr gut<sup>59</sup>. Und wie relativ die Produkte und Aussagen von Google oder Apple sind, kann man an diesem jüngsten Fall sehen, wo sich der „Inkognito-Modus“ als etwas völlig anderes erweist, was dieser vorgibt<sup>60</sup>.

Wer bislang unbedarft seine Daten mit den Herstellern oder den sogenannten sozialen Medien geteilt hat, der hat aus meiner Sicht kein Argument, etwas gegen die Corona-Warning-App zu sagen.

Nun mag man aber auch einwenden, dass Google nunmal keine Polizei oder Ermittlungsbehörden hat, die einen morgens früh an der Haustür begrüßen.

Auf der anderen Seite rettet man mit der Nutzung der App möglicherweise wirklich Leben. In ganz Australien führte die App zu einer einzigen (!) Warnung<sup>61</sup>. Wie wertvoll ist nur ein Menschenleben? Diese Abwägung kann nur und muß auch jeder für sich treffen.

Ich weiß nur, dass es niemals dazu kommen darf - eine Organisation oder ein Behörde diese Entscheidung nie einem abnehmen dürfen.

## Es gibt Wichtigeres als Apps

Vielleicht sollten wir beginnen den Erfolg einer App oder Projektes unter einem anderen Licht zu betrachten. Dazu bringe ich nur ein Vergleich ins Spiel. Betrachten wir uns die Fachanwendung mit dem Namen DEMIS, Deutsches Elektronisches Melde- und Informationssystem für den Infektionsschutz<sup>62</sup>.

---

<sup>59</sup> <https://www.youtube.com/watch?v=qIq17DeAc1M>

<sup>60</sup> <https://www.heise.de/news/Datensammelei-trotz-Inkognito-Modus-Google-soll-Privatsphaere-verletzen-4772637.html>

<sup>61</sup> <https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant>

<sup>62</sup> [https://www.rki.de/DE/Content/Infekt/IfSG/DEMIS/DEMIS\\_node.html](https://www.rki.de/DE/Content/Infekt/IfSG/DEMIS/DEMIS_node.html)

Seit 2016 sind bislang 5.7 Mio EUR als Projektsumme regelrecht verbrannt, denn diese Mittel wurden zum größten Teil zur Finanzierung von Planstellen eingesetzt<sup>63</sup>.

Start der App? Unbekannt. Liegt überhaupt Code vor? Ebenfalls unbekannt. Ende 2020 soll es nach einigen Quellen so weit sein, andere Quellen sagen etwas von 2022. Es könnte aber auch noch viel später werden. Die Website verrät nur, dass es 2019 erst ein erstes Treffen des DEMIS Planungsrates statt fand. Leider handelt es sich dabei auch um den letzten Eintrag in der Rubrik „Aktuelles“ auf der Projektwebsite<sup>64</sup>.

Betrachten wir uns den bisherigen Umgang der Meldezahlen und die Art und Weise wie diese teilweise per Fax oder Excel Tabellen verarbeitet werden. Fax und Excel! Das eine ist eine Entwicklung aus der Mitte des 19. Jahrhunderts, die andere aus den den 80er Jahren des 20. Jahrhunderts. Nur kurz zur Orientierung: Wir befinden uns aktuell im 21. Jahrhundert.

In aufwändigen Forecast-Modellen werden die ankommenden Daten beim RKI bereinigt, amendiert und rückwirkend „geglättet“ damit zum Beispiel die Schwankungen zu Wochenenden heraus gerechnet werden können? Warum ist niemand in der Lage, stündlich bis hinunter auf die Landkreise und Städte eine Übersicht der wichtigsten Kennzahlen anzubieten? So wie es Pavel Meyer auf seiner Seite versucht<sup>65</sup>.

Und Nein, bitte jetzt kein Bashing auf unsere föderalen Strukturen. Diese sind sehr gut und möglicherweise mit ein Grund dafür, dass es uns im Vergleich zu anderen Ländern so gut geht. Dazu reicht nur ein Blick in jene Länder, wo es zentralisierte Gesundheitssysteme gibt. Meine englischen Freunde, obwohl so stolz auf Ihre NHS, blicken durchaus neidisch auf unsere dezentrale Strukturen.

Was ist erfolgreicher? Eine in kürzester Zeit als Open Source und in bestmöglicher Transparenz und Datenschutz hergestellte Corona-Warning-App mitsamt der Server-Infrastruktur dahinter oder ein dahinsiechendes, intransparentes Projekt, das von der Realität kalt erwischt und überholt wurde? Digitalisierung wurde bislang eher stiefmütterlich und wenn, dann komplett falsch behandelt. Private-Public Partnerschaften und Compliance als Feigenblätter für Vitamin-B und einem Abgreifen lukrativer und steuermittelfinanzierter Projekte.

Ich wünschte die FAZ hätte uns mit diesem Artikel „Wieder eine Chance vertan: Die deutsche

---

<sup>63</sup> <https://dip21.bundestag.de/dip21/btd/19/188/1918831.pdf>

<sup>64</sup> [https://www.rki.de/DE/Content/Infekt/EpidBull/Archiv/2019/Ausgaben/08\\_19.pdf?\\_\\_blob=publicationFile](https://www.rki.de/DE/Content/Infekt/EpidBull/Archiv/2019/Ausgaben/08_19.pdf?__blob=publicationFile)

<sup>65</sup> <https://pavelmayer.de/covid/risks/>

Corona-Warn-App“ verschont<sup>66</sup>.

### **Ein Wettrüsten beginnt**

Wir stehen erst am Anfang von etwas, was unsere Zivilisation zuletzt mit der Pest im Mittelalter erlebt hat. Solange es keine wirksame Therapie oder ein Impfmittel gibt, wird Corona Bestandteil in unserem Leben bleiben<sup>67</sup>.

Bedroht COVID-19 Leben und Gesundheit, so bedroht eine Tracing-App unser Zusammenleben.

Das Wissen, ob jemand COVID-19 hat oder demnächst bekommen wird, wird zur wirtschaftlichen Existenzfrage. Am Beispiel des Coesfelder Schlachtbetriebes mit seinen mutmaßlich prekär Beschäftigten wird das sehr gut deutlich. Hätte das Unternehmen einen Wissensvorsprung von nur 1-2 Tagen wäre die Geschichte womöglich anders verlaufen. Welchen Aufwand und Maßnahmen hätte das Unternehmen ergriffen, nicht plötzlich derart prominent in den Medien zu stehen und eine ganze Region in den erneuten Lock-Down zu bringen?

Unternehmen werden Maßnahmen ergreifen, um an dieses Wissen zu gelangen. Legale, grenzwertige und grenzüberschreitende. Im Gegenzug werden Erkrankte mit beginnenden Symptomen aus Ihrer Lage Profit schlagen und einen Gang zum Arzt oder Gesundheitsamt möglichst lange hinauszögern, damit Ihre Smartphones gewinnbringend zur „Anwendung“ an Mitbewerbern oder Mitmenschen kommen können.

---

<sup>66</sup> <https://www.faz.net/aktuell/wirtschaft/digitec/digitalisierung-die-geschichte-der-deutschen-corona-warn-app-16796691.html>

<sup>67</sup> <https://www.youtube.com/watch?v=3z0gnXgK8Do>

## **Änderungsverzeichnis**

### **Update 20.05.2020**

Veröffentlichung des ersten Teils im Kuketz-Forum

### **Update 23.05.2020**

Veröffentlichung des zweiten Teils im Kuketz-Forum

### **Update 30.05.2020**

Veröffentlichung des dritten Teils im Kuketz-Forum

### **Update 13.08.2020**

Überführung der Artikel-Serie in den eigenen Blog. Zahlreiche Formatierungen- und Rechtschreibkorrekturen. Erstellen einer englischen Übersetzung.

### **Update 26.04.2021**

Vorbereitung für pandoc zur Automatischen PDF-Erzeugung. Überschriften eingerückt, kleinere Textanpassungen, Unicode-Sonderzeichen entfernt und ein Änderungsverzeichnis am Ende des letzten Teiles hinzugefügt.