Fokusgruppe Cybersecurity im digitalHUB Aachen e.V.

digitalCHURCH - Jülicher Strasse 72a – D-52070 Aachen

Tel. +49 241 149 46 0

E-Mail: fokusgruppe@plesnik.de
https://aachen.digital/digitalhub-aachen/fokusgruppen/fokusgruppe-cyber-security/

Social Distance Scanner

Mit Digitalisierung und IT-Sicherheit gegen „Corona“

1 Metadaten

1.1 Inhalt

1.2 Versionierung

Version: 1.01
Stand: 14.04.2020

1.3 Copyright / Vertraulichkeit

2 Abstract

Zur Eindämmung der COVID-19-Pandemie („Corona“) ist das Wissen um Kontakte zu infizierten Personen von entscheidender Bedeutung. Aufgrund der Schwierigkeit, solche Kontakte zurückzuverfolgen, kommen vermehrt Vorschläge auf, das Potenzial existierender Technologien wie Smartphones für diesen Zweck zu nutzen.

Die physische Nähe von Personen untereinander könnte auf diese Art automatisiert festgestellt und Infektionswege ausgewertet werden. Dies könnte nicht nur für die aktuelle COVID-19-Situation, sondern auch für zukünftige Pandemien entscheidend dazu beitragen, die Ausbreitung zu verlangsamen.

Um dem Missbrauch einer flächendeckenden Überwachung von Bürgern vorzubeugen, müssen beim Einsatz solcher Tracking-Technologien Privatsphäre, Datenschutz und IT-Sicherheit von Beginn an und im Sinne der Benutzer berücksichtigt werden.

Generell sind zwei wesentliche Anwendungsfälle bzw. Use-Cases zu berücksichtigen: Die statistische Gesamtbetrachtung, die eine globale Bewertung der Pandemieentwicklung und -ausbreitung ermöglicht und die individuelle Bewertung des persönlichen Infektions-Risikos für den einzelnen Nutzer.

Die Fokusgruppe Cybersecurity des digitalHUB Aachen, ein Zusammenschluss von IT-Sicherheitsspezialisten aus Unternehmen und Organisationen der Aachener Region, hat es sich zum Ziel gesetzt, die Entwicklung datenschutz- und IT-sicherheitskonformer Tracking-Lösungen zu unterstützen und vorgeschlagene Ansätze diesbezüglich zu bewerten.

Daraus ergeben sich eine Reihe von Anforderungen, die bei der Entwicklung zu beachten sind. Aus der Fokusgruppe heraus wurde das hier vorliegende Diskussions-Papier erstellt, anhand dessen nun im Verlauf der weiteren Arbeit diskutiert werden kann, wie man eine derartige App und deren zentrale Datenhaltung aufbauen könnte, um die Persönlichkeitsrechte der Nutzer zu wahren. Dazu stellt das Dokument verschiedene, technisch denkbare Lösungsansätze vor und bewertet die jeweiligen Vor- und Nachteile.

Mit diesem Wissen und anstehenden Diskussionspunkten möchte sich die Gruppe nun in die Entwicklung derartiger Lösungen einbringen. Hierbei sollen auch andere, sich derzeit in der Entwicklung befindliche und in den Medien diskutierte Lösungsansätze genauer betrachtet, diskutiert und bewertet und diesen Gruppen eine Zusammenarbeit angeboten werden. Ziel ist es, die Expertise der Fokusgruppe Cybersecurity im Bereich der IT-Sicherheit und des Datenschutzes für den Nutzer in die App einfließen zu lassen. Die Gruppe geht davon aus, dass es unabhängig von bereits auf dem Markt befindlicher Apps Gründe geben wird, diese um weitere Funktionen zu erweitern und somit stetig einen Beitrag an diesen Entwicklungen leisten zu können.

Das Dokument erhebt nicht den Anspruch, alle rechtlichen, technischen und organisatorischen Aspekte vollumfänglich und abschließend zu beschreiben, sondern wird laufend fortgeschrieben (Work in Progress). Die Fokusgruppe lädt dazu ein, hierzu in Dialog zu treten (Request for Comments).

3 Ausgangslage und Motivation

Der Ausbruch des SARS-CoV-2-Virus („Corona“) hat zu Beginn des Jahres 2020 eine weltweite Pandemie mit weitreichenden Folgen für die Gesundheit der Menschen, das soziale, gesellschaftliche und öffentliche Leben sowie für die Wirtschaft ausgelöst. In nahezu allen Staaten der Welt werden Anstrengungen unternommen, die Ausbreitung der Viruserkrankung zu verlangsamen und einzudämmen, um die jeweiligen Bevölkerungen bestmöglich im Fall eines gesundheitlich kritischen Verlaufes versorgen zu können. Da bisher weder Impfstoff noch konkrete Heilmittel entwickelt worden sind, beschränkt sich die Behandlung bei schweren Krankheitsverläufen i.d.R. auf eine intensivmedizinische Betreuung mit Beatmungsgeräten. Während eine Infektion bei der überwiegenden Zahl der Personen sehr mild mit geringen oder gar keinen spürbaren Symptomen verläuft, sind gerade ältere Menschen mit Vorerkrankungen bzw. Personen mit einem geschwächten Immunsystem besonders gefährdet. Als eine wesentliche Maßnahme zur Eindämmung der Infiziertenzahlen haben viele Staaten Ausgangs- bzw. Kontaktverbote erlassen und das öffentliche Leben ist bzw. wird vielerorts in den Monaten März / April 2020 fast vollständig zum Erliegen gekommen sein bzw. kommen. Die Maßnahmen wie Ausgangsbeschränkungen und Kontaktsperren können aus vielerlei Gründen nicht langfristig aufrechterhalten werden. Daher werden Maßnahmen diskutiert, wie diese verantwortungsvoll zurückgenommen und gleichzeitig ein erneutes bzw. weiteres Ansteigen der Infizierungen auf ein vertretbares Maß reduziert werden können. Hier wird u.a. die Auswertung von Mobilfunk-Daten diskutiert, wie sie offenbar mit einigem Erfolg in Süd-Korea durchgeführt wird. In Kombination mit einer dort sehr hohen Anzahl von Tests der Menschen auf Antikörper gegen das Virus wird hierbei versucht, die Kontaktpersonen von Infizierten durch Auswertung der Geo-Daten der Smartphones zu ermitteln. Bei einem positiv auf „Corona“ getesteten Menschen können so automatisiert die vermuteten Kontaktpersonen über deren Smartphones über eine potentielle Infizierung benachrichtigt und zu einem Test bzw. zum Gang in die Quarantäne aufgefordert werden. Dieses Verfahren ist aus rechtsstaatlicher Sicht und im Hinblick auf Datenschutz und Privatsphäre-Aspekte im höchsten Maß kritisch zu sehen und stößt u.a. in der Bundesrepublik Deutschland auf berechtigten Widerstand.

Zu befürchten ist, dass mit dem hehren Ziel, Menschenleben zu schützen, wesentliche Grundrechte temporär oder im schlimmsten Fall dauerhaft ausgehebelt und der bzw. die Staaten einmal gewährte Überwachungsmöglichkeiten nicht mehr zurückgefahren werden. Dennoch könnte eine von den Menschen **freiwillig** installierte App, die die Kontakte zu anderen Smartphones im Nahbereich aufzeichnet und datenschutzkonform sowie aus Security-Sicht sicher speichert, dazu dienen, aktuell bzw. nachträglich festgestellte mögliche Infektionswege und -risiken aufzuzeigen. Die hierbei erhobenen Daten müssen absolut vertraulich und pseudonymisiert[1] erhoben und verarbeitet werden, sodass aus den besonders schützenswerten Gesundheitsdaten keinerlei Nachteil für die Betroffenen resultieren kann. Das vorliegende Dokument soll die Möglichkeiten der technischen, organisatorischen und rechtlichen Ausgestaltung einer solchen App aufzeigen und diskutieren. Im Gutfall soll die Diskussion zu einer kurzfristigen Entwicklung eines solchen Systems führen bzw. zumindest dazu beitragen.

[1] siehe z.B. https://www.datenschutz-notizen.de/unterschied-zwischen-anonymisierung-pseudonymisierung-und-verschluesselung-2916984/

4 Abstrakte Umsetzungsidee

In der Fokusgruppe wurde zunächst die nachfolgend näher beschriebene Idee auf Basis der sogenannten Bluetooth UUID[2]s (Universally Unique Identifier) diskutiert und im weiteren Verlauf durch Optimierungen und Alternativkonzepte verfeinert. So wird in den folgenden Unterkapiteln zunächst die ursprüngliche und naheliegende Idee der Auswertung der UUID dazu verwendet, das grundsätzliche Konzept mit möglichen Missbrauchsszenarien zu modellieren. Wenn dort also von einer UUID als Identifier gesprochen wird, ist dies bei Anwendung einer anderen Lösungsidee, wie in Kapitel 5 näher beschrieben und hinsichtlich der Vor-und Nachteile diskutiert, auszutauschen.

4.1 Technische Komponenten

Praktisch alle Menschen führen heutzutage ein Smartphone quasi ständig am Körper mit. Dies, vor allem, wenn sie das Haus verlassen und sich in der Öffentlichkeit bewegen. Die meisten heute aktuell verwendeten Smartphones sind mit Bluetooth Sender- und Empfängern ausgestattet. Hierbei kommt in aktuelleren Geräten der Bluetooth Standard Low Energy[3] (BLE) zum Einsatz, welcher bei relativ niedrigem Stromverbrauch im Nahbereich eine hohe Funktionalität und Kommunikationsfähigkeit besitzt. Eine aktive Bluetooth-Kommunikation basiert auf dem Prinzip des Pairings von Geräten. Damit zwei Geräte erfolgreich miteinander kommunizieren können, müssen sie sich gegenseitig einmalig autorisieren. Ist dieser Vorgang erfolgreich abgeschlossen, werden die beiden Geräte anschließend immer wieder prüfen, ob sie sich in Funkreichweite zueinander befinden und dann wieder (ggf. ungefragt) eine Verbindung herstellen. Damit dieser Mechanismus funktionieren kann, senden die Geräte bei aktivierter Bluetooth-Funktion ständig ihre gerätespezifische Kennung aus (im Advertising-Modus[4] zwischen 20 ms und 10,24 s). Diese Kennung sollte weltweit eindeutig und statisch sein bzw. es ist aufgrund der großen Schlüssellänge des Identifiers davon auszugehen, dass es in der Praxis nur sehr selten zu Dubletten kommt. Es gibt auch Random-IDs, die nur für einen Power-Zyklus gelten und nur in bestimmten Use-Cases verwendbar sind.

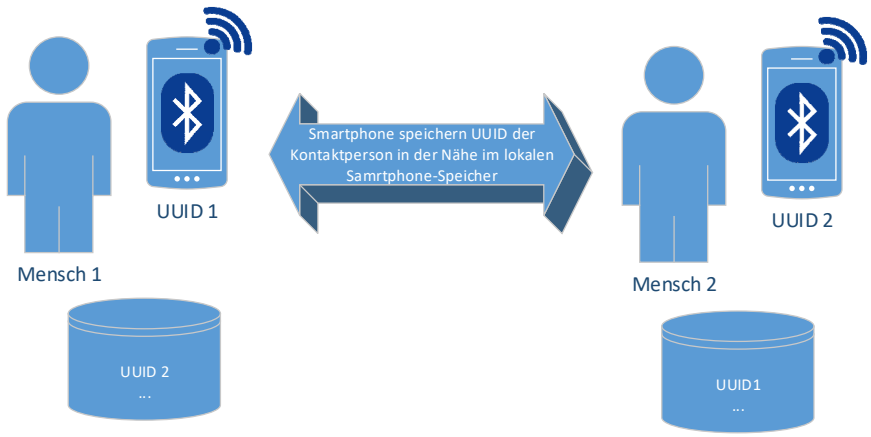

Abbildung 1: Ablegen der gescannten UUID des Gegenübers lokal in der App

[2] siehe z.B. https://de.wikipedia.org/wiki/Universally_Unique_Identifier
[3] siehe z.B. https://de.wikipedia.org/wiki/Bluetooth_Low_Energy
[4] siehe z.B. https://www.elektroniknet.de/elektronik/kommunikation/bluetooth-low-energy-in-smartphones-wie-funktioniert-das-103061-Seite-2.html

Die UUID hat noch eine weitere Eigenschaft. Sie kann ohne weitere geräte- oder nutzerspezifische Daten nicht einer bestimmten Person (Nutzer) zugeordnet werden. Zudem ist in ihr keinerlei Geo-spezifische Information enthalten.

4.1.1 Scanner-Komponente

Da die Bluetooth-fähigen Devices also ständig ihre eigene UUID als Beacon im Nahbereich (wenige Meter) aussenden, können andere Geräte diese erfassen (scannen) und anhand der Signalstärke (bzw. ggf. vermutlich über Laufzeit des Signals) sogar eine ungefähre Abschätzung vornehmen, wie weit das gerade gescannte Gerät entfernt ist. Dieser Mechanismus funktioniert wohlgemerkt ohne dass sich die Geräte vorher bereits begegnet sind bzw. jemals eine (gekoppelte) Verbindung bestanden hat. Erst wenn beide Geräte von den jeweiligen Nutzern in den Pairing-Modus versetzt würden, könnte eine tatsächliche Kopplung stattfinden.

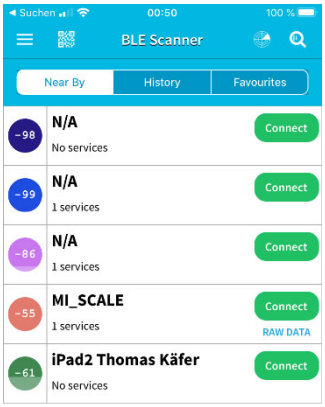

Abbildung 2: Screenshot BLE Scanner App

Dies wird hier aber gar nicht benötigt. Es reicht, jede in der Umgebung gescannte UUID im lokalen Speicher des Smartphones mit einem absoluten Datumsstempel abzulegen. Hierbei sollten die Dauer (ohne genaue absolute Uhrzeiten) sowie die Verbindungsparameter (Signalstärke bzw. ermittelte/abgeschätzte Distanz) und ein Score-Wert als Indikator für das Infektionsrisiko hinterlegt werden (siehe dazu auch Kapitel 4.5.5).

Auf diese Weise erstellt das Smartphone eine kontinuierliche Liste von allen anderen Bluetooth-Devices, mit denen es im näheren Umfeld in Kontakt gekommen ist. Die Messung der Distanz ist beim aktuellen Standard BLE 4.X bzw. 5.0 nur im Meter-Bereich möglich. Mit der kommenden Generation 5.1 soll eine Distanzmessung im Zentimeterbereich incl. Richtungserkennung möglich sein (was aber für die jetzige Lage nicht nutzbar ist). Beim Scannen werden auch viele Bluetooth-Geräte erfasst, die nicht zu einem Smartphone gehören (andere Computer, Headsets, Navigationssysteme, Home-Automatisation usw.). Dieser Beifang ist unkritisch und unerheblich, da er nur lokal oder gar nicht gespeichert wird. Ggf. kann durch Erkennung der Bluetooth-Profile der potentiellen Kommunikationspartner erkannt werden, ob es sich überhaupt um Smartphones handelt. Bei sicherer Erkennung eines Gerätes, welches kein Smartphone ist, könnte diese UUID direkt ausgeblendet werden.

Durch geeignete Verschlüsselungsmaßnahmen wird zudem sichergestellt, dass diese Daten nur für das Smartphone bzw. dessen Benutzer selbst lesbar sind und somit auch nicht nachträglich unlegitimiert zum Nachteil des Benutzers oder seiner Kontaktpartner verwendet werden können (z.B. zur Erstellung von Bewegungs- und Kommunikationsprofilen). Dieser Scan- und Protokolliervorgang funktioniert unabhängig von einer App bei der Gegenseite. Sofern mit einer nicht veränderbaren statischen UUID gearbeitet wird, kann ein Nutzer auch später noch die App installieren und seine Status-Werte hochladen (siehe nachfolgende Kapitel). Frühere Kontakte partizipieren dann nachträglich von seinem Upload.

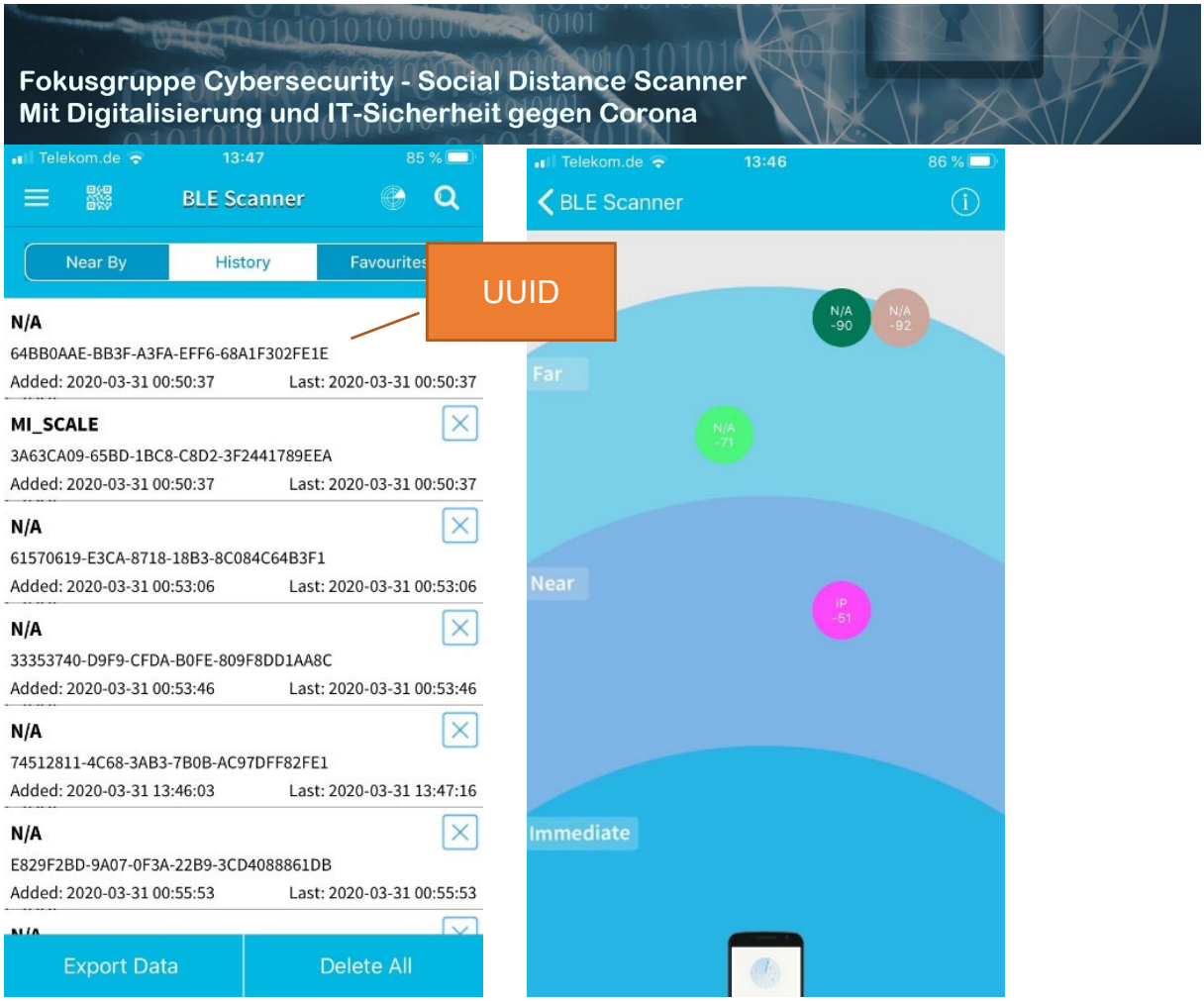

Abbildung 3: Screenshots aus App BLE Scanner

4.1.2 Melde-Komponente

Die Smartphones bzw. die entsprechende App bietet neben der Scanner-Funktion eine Meldefunktion an, mit der der User seinen persönlichen und aktuellen Gesundheitszustand erfassen und an eine zentrale Serverstelle melden kann. Dazu gehört auch, eine überstandene Erkrankung zu melden. Hierbei muss im Status bzw. bei der nachfolgenden Berechnung des Score-Werts (siehe Kapitel 4.1.3) unterschieden werden, ob die Meldung unqualifiziert und unverifiziert vom Nutzer selbst kommt oder durch ein negatives Testergebnis bestätigt wurde (siehe Test-Komponente). Durch Plausibilitätsprüfungen der historischen Daten kann der Wahrheitsgehalt der Aussagen bewertet werden.

Beispiel: Eine Meldung einer überstandenen Krankheit ohne Testergebnis wird weniger stark als „wahr immun“ gewertet als eine eher typische Historie mit Kontakten zu Infizierten, einer nachfolgend gemeldeten Erkrankung mit Symptomen und dann (später) einem kommunizierten und via Test verifizierten Negativ-Ergebnis.

Dies erfolgt wiederum allein über die UUID des Gerätes und ohne weitere personenbezogene Daten. D.h., der Nutzer gibt in seinem Gerät ein, ob er z.B. Symptome feststellt, Kontakt zu einem bestätigten Infektionsfall hatte oder sogar selbst positiv oder negativ auf das SARS-CoV-2-Virus getestet wurde. Dieser Status wird zusammen mit dem zugehörigen Datums- und Zeitstempel (Anmerkung: Die Verwendung eines Zeitstempels ist Datenschutztechnisch nicht unkritisch) an den Server übermittelt.

Dort entsteht nun ein Datensatz zur UUID des Nutzers (bzw. seines Smartphones) mit dessen Infektionshistorie. Diese Daten sind anonym (pseudonymisiert) und können ohne weitere Merkmale nicht zu einem Personenbezug aggregiert werden.

Gefahr und Herausforderung: Diesen Personenbezug herzustellen, wäre aber ggf möglich, wenn man die BLE-Kommunikationspartner anderer Geräte (Smart-TVs mit eigener Herstellerdatenbankkopplung, Bezahlvorgänge per BLE an der Supermarktkasse etc.) aus anderen Datenquellen zu denen der „Corona“-App-Datenbank hinzuaggregiert. Dann würden ggf. dort zu den BLE UUID gespeicherte Zusatzinformationen wie Name, Ort, Adressen etc. sozusagen „über die Hintertür“ dazu führen, dass eine Person anschließend über ihre BLE UUID doch identifizierbar wird. Das muss unter allen Umständen verhindert werden.

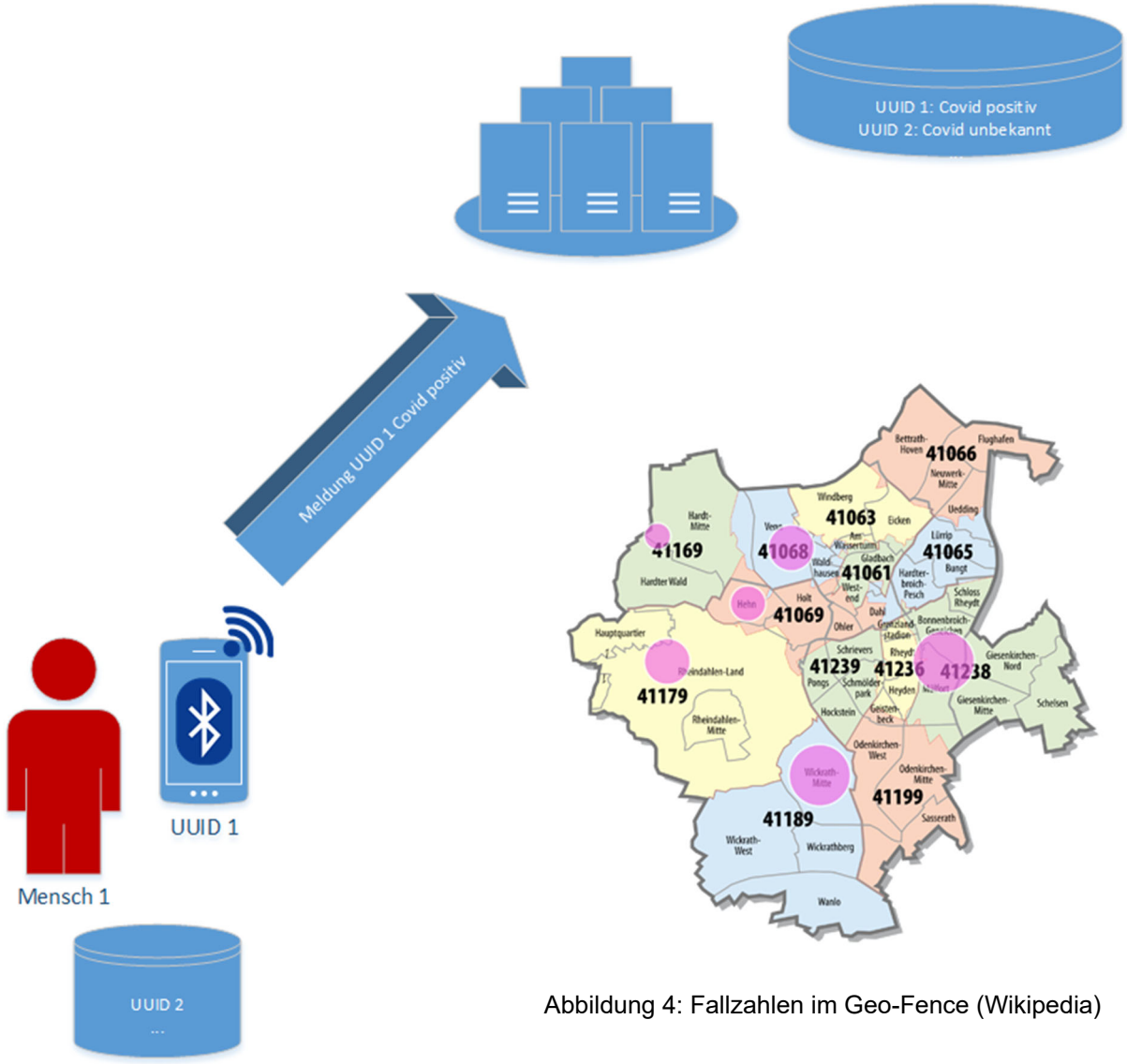

Abbildung 5: Meldung an Datenbank: Mensch 1 (UUID 1) ist Covid positiv getestet

Abbildung 4: Fallzahlen im Geo-Fence (Wikipedia)

Um die Pandemie bzw. deren lokalen Fallzahlen übergeordnet auswerten zu können, wird zur UUID nur ein ausreichend groß gewählter (bewusst ungenauer) Geo-Bereich hinzuaggregiert, sodass man für diese Areale Abschätzungen vornehmen kann, wie hoch die jeweiligen Infizierungsraten sind. Ein datenschutzkonformer ausreichend großer Bereich könnte beispielsweise die Größe eines PLZ-Gebiets der Bundesrepublik Deutschland sein. So könnte man selbst in einer größeren Stadt noch ausreichend genau auf Stadtviertel bezogen Fallzahlen und deren Entwicklung monitoren, ohne eine einzelne Person eindeutig identifizieren zu können.

4.1.3 Abfrage-Komponente

Jedes Smartphone kann nun regelmäßig seine protokollierten Bluetooth-Kontakt-UUIDs gegen die zentrale Server-Datenbank prüfen. Gibt es zu einer lokal getrackten UUID einen passenden Eintrag in der Server-Datenbank, so wird die Historie der dort gespeicherten Daten (Infektionsverlauf) incl. Score-Wert (Grad des Infektionsrisikos) an das abfragende Smartphone übertragen.

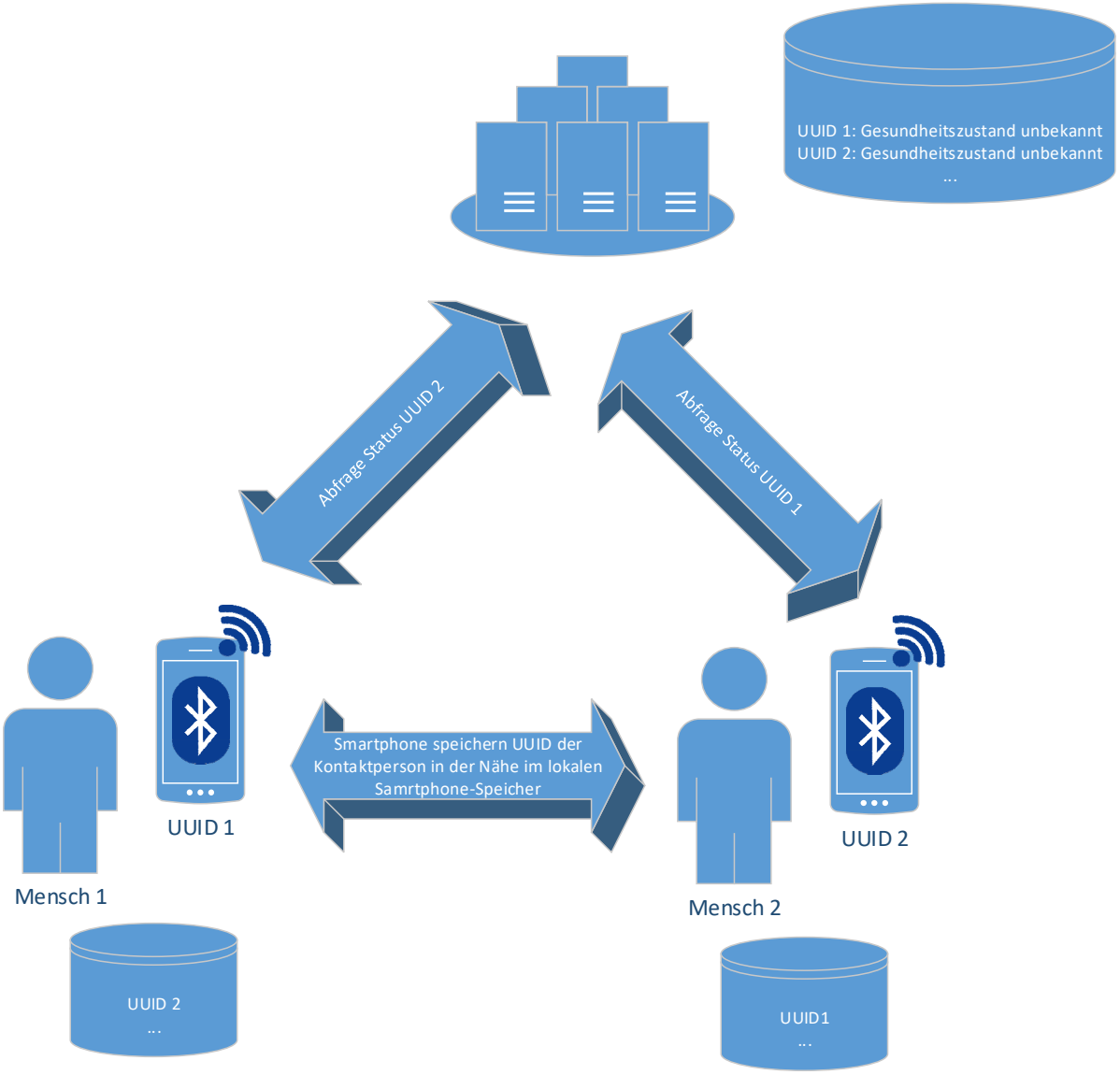

Abbildung 6: Abfrage der Gesundheitsdaten des aktuellen Kontaktpartners

Die App im Smartphone erhält somit zeitnah bzw. rückwirkend eine Information, ob ein Bluetooth-Kontakt potentiell oder sicher mit „Corona“ infiziert ist bzw. zum Zeitpunkt eines früheren Kontakts war. Anhand eines von Virologen festgelegten Zeitablaufs kann die App (rückwirkend) errechnen, ob der entsprechende Kontakt zum Zeitpunkt des Aufeinandertreffens potentiell ansteckend war.

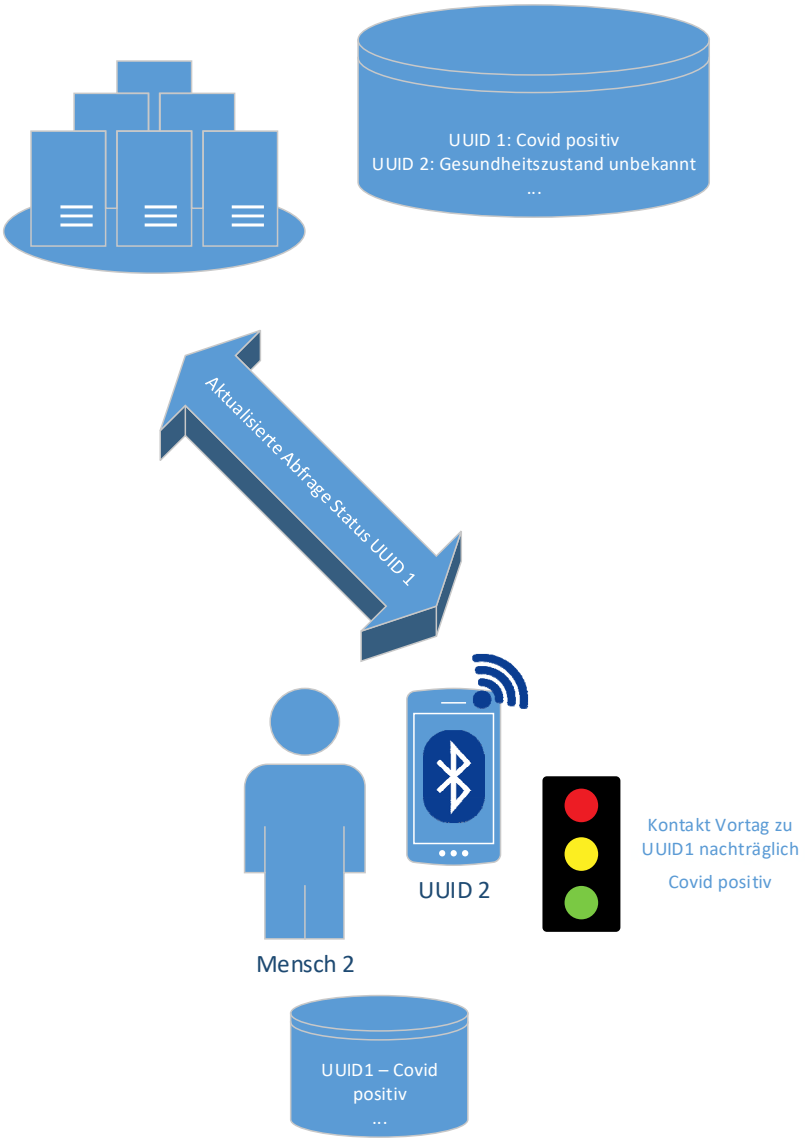

Abbildung 7: Nachträgliche Aktualisierung des Status von Kontakt UUID1

Hier können Wahrscheinlichkeitsberechnungen sowie Anzahl, Distanzen und Dauer von ggf. wiederkehrenden Kontakten mit derselben UUID dazu führen, dass man einen individuellen Score-Wert für dieses Kontaktpärchen errechnet. Dieser Score-Wert reflektiert dann die Wahrscheinlichkeit dafür, dass sich der Nutzer des Smartphones bei dieser Kontaktperson angesteckt haben könnte. Hierbei könnten Datum und ggf. Zeit einer wahrscheinlichen Ansteckung errechnet und angezeigt werden. Wohlgemerkt ist dieser Score-Wert nur eine Wahrscheinlichkeit und bietet weder eine Gewissheit für eine Infektion noch für das Gegenteil. Aber sie hilft enorm, das eigene Infektionsrisiko laufend bewerten zu können.

4.1.4 Broadcast-Komponente

Wenn eine Person mehrfach Kontakt zu potentiell infizierten Personen hatte und deren Score-Wert entsprechend ansteigt, so liegt es im Interesse aller, dass diese Person dazu aufgefordert und motiviert wird, sich selbst testen zu lassen bzw. sich in Quarantäne zu begeben.

Der Staat bzw. die Gesundheitsbehörden haben durch das forcierte Melden via App die Möglichkeit, den Nutzer auf die Dringlichkeit eines eigenen, aktuellen Tests hinzuweisen, ohne eine weitere Repressalienmöglichkeit zu haben. Dies sollte (automatisiert) zusammen mit Informationen und Kontaktdaten der Gesundheitsbehörden und in der Nähe liegenden Testcenter an die App bzw. den Nutzer der App gemeldet bzw. von dieser anonym abgerufen werden können (Pull statt Push).

4.1.5 Test-Komponente

Testergebnisse von tatsächlich erfolgten Tests auf das SARS-CoV-2-Virus sollten manipulationssicher und wiederum anonymisiert an das Smartphone des Betroffenen gemeldet werden können. Das Testen muss anonym, kostenlos und mehrfach wiederholbar sein. Hierzu könnte der Test selber vollkommen ohne Angabe von Namen und weiteren personenbezogenen Merkmalen erfolgen und als Identifier wiederum die UUID des Smartphones genutzt werden (App zeigt UUID als Text oder QR-Code zum Scannen vor Ort beim Test auf dem Bildschirm an.).

Jetzt kann das Testergebnis zeitversetzt vom Labor der UUID auf dem Server zugeordnet und dort hochgeladen werden.

Durch Einsatz geeigneter Signierverfahren (Digitale Signatur mit dem Private Key des Smartphones, Hashing-Verfahren incl. SALT o.ä. oder durch Einsatz der Blockchain-Technologie) könnte sichergestellt werden, dass ein Befund nur durch diese initiale und explizite Legitimierung durch den User seinem Datensatz auf dem Server zugeordnet wird. Das würde einen Missbrauch durch unbewusst oder bewusst falsch hochgeladener Testergebnisse verhindern. Gleichzeitig unterbindet dies auch die Möglichkeit, dass der Nutzer selber für sich gute (negative) Testbefunde seinem Account zuordnet und sich somit fälschlicherweise als „gesund“ ausgibt.

4.1.6 Monitor-Komponente

Für die Gesundheitsbehörden ist es enorm wichtig, schnell und räumlich weitestgehend präzise Daten über den Infektionsstand der Bevölkerung abrufen zu können. Dies ermöglicht zum einen eine Bewertung über die Entwicklung der Neuinfektionen genauso wie über die Heilungen bzw. den Grad der Herdenimmunität. Des Weiteren ist auch ein Forecast für die zu erwartende Belegungszahl von Intensivbetten und Beatmungsgeräten (regional) zu erhalten.

Ideal aus Sicht der Forschung wäre eine Weltkarte mit Reisewegen. Aber auch hierbei muss unbedingt auf die Einhaltung des Datenschutzes geachtet werden.

Durch die Anonymisierung der Daten ist es den Gesundheitsbehörden bzw. der Exekutive nicht möglich, einzelne Personen zu identifizieren, um diese ggf. mit Zwangsmaßnahmen in Quarantäne zu stecken.

Das ist mit diesem Konzept explizit auch nicht gewünscht, da es in letzter Konsequenz nicht nur einen erheblichen Eingriff in die Privatsphäre und Freiheit des Einzelnen darstellt, sondern in ungünstigen gesellschaftlichen bzw.- staatlichen Konstellationen zu einem totalitären Überwachungsstaat führen kann. Eine Brandmarkung des Einzelnen auf Basis seines Score-Wertes oder einer tatsächlich festgestellten Infektion muss vermieden werden – dies auch trotz des zunächst hehren Ziels, damit andere Menschen zu schützen.

4.1.7 Server-Komponente

Unzweifelhaft muss es eine Server-Komponente in Form einer zentralen Datenbank geben, die es erlaubt, die mit der UUID eines jeden App-Nutzers (Primärschlüssel) verknüpften Daten über dessen Gesundheitszustand hochladen und speichern zu können.

Der Upload muss genauso wie der nachfolgende Download von Daten ohne jegliche User-Registrierung vollkommen anonym erfolgen. Hierbei besteht die Herausforderung darin, auf der einen Seite die Anonymität zu gewährleisten (keine Protokollierung von TCP/IP- und MAC-Adressen sowie Verbindungsdaten etc.) und gleichzeitig ein Flooden mit Falschinformationen (durch Hacker oder Schad-Software) zu verhindern. Dies könnte z.B. durch den Einsatz eines Digitalen Signaturverfahrens (PKI[5]) nach dem aktuellen Stand der Technik erfolgen. Hierbei wird in der App auf jedem Smartphone ein Paar aus einem öffentlichen und privaten Schlüssel (Signatur) erzeugt und lokal gespeichert. Der öffentliche Schlüssel wird beim ersten Kontakt zum Server im Datensatz der jeweiligen UUID abgelegt.

Jede weitere Kommunikation mit einem Schreibzugriff auf die Server-Daten erfolgt nur mit der Signatur des privaten Schlüssels der App / des Smartphones. Die Server-Komponente kann nun mit dem öffentlichen Schlüssel überprüfen, ob die Nachricht tatsächlich vom legitimierten Smartphone kommt. Solange der private Schlüssel im Smartphone sicher aufbewahrt und nicht ausgelesen werden kann, ist eine Fälschung der Datenpakete durch Dritte ausgeschlossen.

Für die Legitimierung Dritter zum begrenzten schreibenden Zugriff auf den Datensatz der UUID kann die App mit Autorisierung des Benutzers zeitlich begrenzte bzw. fallbezogene Berechtigungen Autorisierungscodes ausstellen, mit denen z.B. Test-Ergebnisse von Laboren hochgeladen (bzw. korrigiert) werden können (siehe Kapitel 4.1.5).

Der lesende Zugriff auf die Einträge der UUID im Server erfolgt ohne Autorisierung vollkommen anonym, um die Abfragen anderer Kontaktpartner (Watcher – siehe Kapitel 4.3.3) zu ermöglichen.

Das zentrale Server- bzw. Datenbanksystem muss hierbei von vorneherein so ausgelegt werden, dass es der im Gutfall extrem hohen Anzahl von Datensätzen und Anfragen gerecht wird (verteilte Systeme, Loadbalancing etc.).

[5] PKI: Public Key Infrastruture

4.2 Statistische Auswertungsmöglichkeiten

In Bezug auf die statistischen Auswertungsmöglichkeiten bzw. einer übergeordneten Sicht auf den Verlauf der Infizierungen gibt es unterschiedliche zu erwartenden Anforderungen bzw. Ausprägungen, die wiederum unter dem Gesichtspunkt des Seuchenschutzes **und** Privatsphäre / Datenschutz zu betrachten sind.

Nicht jede Anforderung in den nachfolgenden Kapiteln kann mit jeder Lösungsidee im Detail gleich gut umgesetzt werden (siehe dazu auch die Bewertungsmatrix in Kapitel 5.7).

4.2.1 Ermittlung der Infizierten-Zahlen

Die einfachste Form der Auswertung ist eine Aufsummierung der Datensätze nach Status. Hierbei kann man durch Auswertung der auf dem Server gespeicherten Tabelle die Datensätze zählen und erhält die Gesamtzahl der Smartphones, die am System teilnehmen. Die Zahl der zugehörigen natürlichen Personen ist maximal gleich groß, in der Realität wird sie jedoch niedriger liegen (z.B. weil eine Person zwei Smartphones benutzt).

Ist zum Identifier ein Gesundheitsstatus hinterlegt, können basierend auf der Gesamtzahl die prozentualen Anteile der infizierten, nicht infizierten und genesenen Personen ermittelt werden. Ein nicht zu vernachlässigender Rest der Datensätze wird keinem Status zuzuordnen sein („Watcher“ ohne eigene hochgeladene Daten).

4.2.2 Ermittlung der absoluten Kontaktzahlen

Bei der Ermittlung der Kontaktzahlen sind zur Einschätzung des Einhaltens von Versammlungs- und Kontaktverboten die Werte pro Identifier interessant, mit denen die zugehörige Person in einem bestimmten Zeitraum in der näheren Umgebung Kontakt hatte. Eine hohe Kontaktzahl in einem engen Zeitfenster deutet dann auf eine Ansammlung von Personen hin. Dies ließe sich analog auch ggf. durch Auswertung von Mobilfunkdaten erreichen (wie mutmaßlich im Beispiel Südkorea).

4.2.3 Ermittlung der konkreten Kontaktzahlen bei Infizierten

Viel wichtiger ist die Ermittlung der Kontakte bei einer (nachträglich) festgestellten Infizierung. Hier ist neben der persönlichen Benachrichtigung der Betroffenen auch eine Gesamtbetrachtung interessant, die Aufschluss darüber gibt, wie viele Kontakte potentiell bei einem Infizierten zu weiteren Infizierungen geführt haben könnte.

4.2.4 Ermittlung der Benutzerbewegungen incl. Lokalisierung

Durch Aggregieren von Standort-Daten zu Identifiern können die einzelnen Personen auch räumlich katalogisiert bzw. kategorisiert werden. Hierbei ist aus Datenschutzgründen besonders zu achten, dass die genauen Positionen so verrauscht werden, dass eine konkrete Lokalisierung verhindert wird. Stattdessen sind ausreichend genaue Cluster zu bilden, die keinen Rückschluss auf das Individuum jedoch auf lokale Ausbreitungsherde ermöglichen.

Je nach Ausprägung sind so auch Reisewege des Virus nachzuvollziehen.

4.3 Organisatorische Fragestellungen

4.3.1 Override-Modus

Zu diskutieren ist, was passiert, wenn eine Person ernsthaft erkrankt und intensiv behandelt werden muss oder gar verstirbt. Hier sollte es eine Möglichkeit geben, dass entsprechend vertrauenswürdige Institutionen (z.B. Ärzte) die Möglichkeit haben, den Status der UUID des Betroffenen entsprechend aktualisieren zu können. Das sollte – solange die Person lebt und entscheidungsfähig ist – nur mit ihrer Erlaubnis passieren. Nach ihrem Tod greifen weder Datenschutz- noch Persönlichkeitsaspekte und hier wäre dem Seuchenschutz dann Vorrang zu gewähren und zu erlauben, dass der Datensatz auch ohne Einwilligung entsprechend aktualisiert wird. Da es in der Datenbank ja keine Zuordnung zwischen UUID und natürlicher Person gibt, kann eine solche außerplanmäßige bzw. nachträgliche Datenaktualisierung nur über das Smartphone des Betroffenen erfolgen.

4.3.2 User-Status

Ein Nutzer der App (Mensch) kann folgende Status haben (Aufzählung nicht abschließend, durch Virologen zu definieren):

- unbekannt oder nicht infiziert
- infiziert und ansteckend
- hat Antikörper / gesund
- geheilt
- ist geimpft
- hat Symptome, ist aber negativ getestet
- tot

4.3.3 User-Level

Ein Mensch kann die App in unterschiedlichen Ausprägungen nutzen:

Watcher: User bezieht Status seiner Kontaktpersonen, kommuniziert bzw. ändert aber seinen Status nicht aktiv.

Player: User lässt sich testen und kommuniziert das Ergebnis bzw. seinen Gesundheitszustand laufend aktualisiert und aktiv.

Der Mehrwert für den Player besteht neben der Tatsache, dass das System nur funktioniert, wenn möglichst viele User „Player“ sind, darin, dass er bei einer überstandenen Krankheit und einer (temporären) Immunität einen Nachweis mit sich führt, der ihm ggf. eine größere Bewegungsfreiheit erlaubt.

Dies führt zu einem diskussionswürdigen Szenario, bei dem z.B. der Zutritt zu einem Geschäft oder einem Gebäude (einfacher) gewährt wird, wenn man eine Freigabe durch einen bestätigten Negativ-Bescheid über sein Smartphone mit sich führt. Das könnte elektronisch gescannt werden. Im Umkehrschluss bedeutet dies, dass Menschen, die die App nicht nutzen, benachteiligt würden. Neben dem daraus resultierenden Missbrauchs-Szenario durch Fälschen günstiger Bescheinigungen kann dies zu einer Stigmatisierung und Ausgrenzung von Menschen führen, die nicht am System teilnehmen.

4.4 Anwendungs- und Missbrauchsszenarien

Bei der Konzeption der Lösung sind von vorneherein intensive Überlegungen anzustellen, wie ein Missbrauch durch Nutzer, Betreiber, staatliche Organisation sowie Hacker möglichst vollständig unterbunden werden kann.

4.4.1 Szenario 1 – Akut Infizierter im Umfeld

Ein akut Infizierter weiß von seiner Infektion, lädt diese Information zum Server hoch und somit ist der Score-Wert seiner UUID entsprechend hoch (schlecht). Nun scannt ein neuer Kontakt in der Umgebung des Infizierten und prüft dessen Status online. Er bekommt sofort eine Warnung, dass ein Infizierter in der Nähe ist. Das kann unmittelbar zu Misstrauen bis hin zu einer Panikreaktion führen. Ist nur eine Person offensichtlich in Reichweite, weiß der neue Kontakt sofort, dass sein Gegenüber mit hoher Wahrscheinlichkeit infiziert ist. Aus Seuchenschutzsicht ist dies gut, aber die mögliche Überreaktion ist wiederum abzuwägen.

Wird der Status nicht sofort abgerufen, so reduziert das zwar die Option für eine Panikreaktion, schützt jedoch auch das Umfeld nicht vor dem Infizierten.

4.4.2 Szenario 2 – Trügerische Sicherheit durch False Negatives

Im aktiven Umfeld werden durch eine aktualisierte Abfrage Kontakte gemeldet, die infiziert waren oder bei denen nur ein geringer Score-Wert auf eine niedrige Infektionswahrscheinlichkeit hinweist. Im Extremfall könnte sogar ein sehr niedriger Score-Wert eine vermeintliche Sicherheit vorgaukeln (durch ein „False-Negative“-Ergebnis bei einem Test). Das bedeutet dann lediglich, dass es keine Anhaltspunkte für eine Infektion gibt (geringes Risiko), aber das ist keine sichere Erkenntnis und könnte zu einer Sorglosigkeit hinsichtlich der Einhaltung von Schutzmaßnahmen führen.

4.4.3 Szenario 3 – Zugangskontrolle am Eingang

Ladenbesitzer könnten am Eingang aktiv scannen, ob Besucher hohe Score-Werte haben und diesen dann den Zutritt verweigern. Damit wird zwar die Seuchengefahr gesenkt, aber die Akzeptanz der User mutmaßlich auch, da sie sich selber aktiv diskreditieren. Das kann bei überempfindlichen Menschen im Umfeld leicht zu Stigmatisierung und Überreaktion führen.

4.4.4 Szenario 4 – Rückverfolgung und Aggregieren mit Zusatzdaten

Die Rückverfolgung bzw. Identifizierung von Personen durch Aggregieren mit weiteren Daten muss verhindert werden.

Beispiel: Beide Kommunikationspartner haben sich am gleichen Tag am selben Ort testen lassen. In häuslicher Gemeinschaft lebenende Personen würden nun über das gleiche Geo-Fence und durch Aufzeichnen von Bewegungsprofilen ggf. identifizierbar.

Des Weiteren muss die Kommunikation von Smartphone mit den Servern verschlüsselt und anonymisiert sein. Der Schutz darf nicht unterwandert und die Kommunikation darf nicht von staatlichen Organisationen mitgelesen werden können.

Die UUID darf nicht in Herstellerverzeichnissen existieren, damit keine Rückschlüsse auf Seriennummern, IMEI[6] oder IP-Adressen möglich sind. Es dürfen keine gerätespezifischen Infos gespeichert werden (z.B „Tom‘s iPhone zusätzlich zur UUID).

4.4.5 Szenario 5 – Auswertung zu Geschäftszwecken

Die massenhafte Auswertung der Serverdaten zu Geschäftszwecken soll unterbleiben. Auf der anderen Seite sollte die statistische Auswertung transparent und für jedermann frei zugänglich sein, um das Vertrauen in dieses System zu erhöhen und den wissenschaftlichen Nutzen zu maximieren.

4.4.6 Szenario 6 – Störung des Dienstes

Die Störung des Dienstes oder gar das Einschleusen von Schad-Code bzw. die Verteilung von Schad-Code (z.B. als Drive-by-Download) muss unterbunden werden. Dies ist durch Härtungsmaßnahmen der Server und durch entsprechende Pen-Tests sicherzustellen. Alle BLE-Geräte, die kein Smartphone mit App sind, werden beim Upload ignoriert. Das Hochladen von gefakten Daten muss verhindert werden (incl. Flooding).

4.5 Kritik, Grenzen und zu erwartenden Probleme

4.5.1 Kritische Nutzermasse

Eine der wesentlichen Herausforderungen ist das Erreichen einer kritischen Masse bei den Nutzerzahlen. Nur bei einer entsprechend hohen Durchdringung in der Gesellschaft hat das Konzept eine Chance, einen echten Mehrwert zu liefern. Bzgl. des Marketings ergibt sich somit die Herausforderung, den Mehrwert und den Sicherheitsgewinn für jeden Bürger deutlich werden zu lassen.

4.5.2 Ausstattungsquote Smartphone

Während bei jüngeren Menschen die Ausstattung mit einem Smartphone und das ständige Mitführen desselbigen als weitestgehend gegeben angesehen werden kann, trifft das für sehr junge Kinder und ältere Personen eher nicht bzw. nicht im gleichen Maße zu. Gerade ältere Personen gehören jedoch offenbar zur Risikogruppe. Des Weiteren sind nationale Unterschiede zu berücksichtigen, da nicht in jedem Land der Besitz eines eigenen Smartphones selbstverständlich ist.

Von Personen, die kein Smartphone besitzen oder mitführen (z.B. in Bereichen, in denen Smartphones verboten sind), sind daher weder statistische Daten zu erwarten noch können diese über die App ihr eigenes Infektionsrisiko abschätzen. Hier sind ggf. alternative Konzepte zu diskutieren, wie beispielsweise die Entwicklung und das (ggfs. kostenlose) Zurverfügungstellung von einfachen Bluetooth-Scannern mit Funkübertragung zum Datenabgleich (Smartphones light, Smartwatches oder proprietäre Geräte.).

4.5.3 Mitführen mehrere Smartphone bzw. Gerätewechsel

Des Weiteren wird es Konstellationen geben, bei dem ein Benutzer zwei Smartphones mitführt (ein dienstliches und ein privates) bzw. innerhalb der für die Infektion interessanten Zeiträume ein Gerätewechsel stattfindet.

[6] IMEI: International Mobile Station Equipment Identity https://de.wikipedia.org/wiki/International_Mobile_Equipment_Identity

Hier muss konzeptionell und durch Funktionen in der Benutzerführung der App ermöglicht werden, veraltete Profile auf Basis der Bluetooth-ID zu löschen bzw. zu übertragen und Smartphones bzw. deren Daten auf einen Status „ignorieren“ oder „veraltet“ zu setzen. Dies ist langfristig vor allem in Bezug auf die Speicherung von Negativ-Befunden relevant, die dem Träger des Smartphones ggf einen Vorteil verschaffen, da er sich mit fremden (historischen Daten des Vorbesitzers) als „geheilt“ oder „immun“ ausweisen kann.

4.5.4 Technologiegrenzen

Die App bzw. der Scan-Vorgang kann die Qualität eines Kontaktes zwischen zwei Menschen nicht zuverlässig bewerten. Nach Aussage eines Virologen ist beispielsweise ein intensiver Kontakt von mehreren Minuten (ca. 15 min) kritischer zu bewerten, als eine flüchtige Begegnung. Zudem kann die App bzw. das Smartphone nicht erkennen, ob tatsächlich eine Kommunikation zwischen den Kontaktpartnern stattgefunden hat, ob sich diese gegenüber gestanden haben oder ob sie ggf. durch Schutzwände gesichert waren (Plexiglas bzw. andere für Funkwellen durchlässige Materialien).

4.5.5 Scoring und Wahrscheinlichkeiten

Wenn im vorliegenden Dokument von Score-Werten gesprochen wird, so ist hiermit gemeint, dass die Bewertung eines Infektionsrisikos auf Basis von Kontaktdaten mit der Systemungenauigkeit „Smartphone“ bzw. „Bluetooth“ nur als Abschätzung bzw. Wahrscheinlichkeit angeben kann und einem hohen Unsicherheitsfaktor unterliegt. Dennoch ist diese Abschätzung hilfreich und es muss ein Maß gefunden werden, Kontakte und Risiken qualitativ und quantitativ zu bewerten und somit auch messbar zu machen. Zu diskutieren und festzulegen ist dabei auch, wer diese Maßstäbe festlegt, damit diese nachher automatisiert im System errechnet werden können.

4.5.6 Herausforderung Trennung von Nutz- und Verbindungsdaten

Einer der wichtigsten Punkte bei der Realisierung eines durchgängigen Daten- und Persönlichkeitsschutzes wird die Trennung von Verbindungs-Daten und Kommunikations-Logs von den eigentlichen Nutzdaten sein. Das wird technisch wie organisatorisch schwierig sein. Gerade wenn der Betrieb der Server-Komponente in staatliche Hand gelegt wird, darf ein (späterer) Interessenkonflikt unterstellt werden, diese Daten auch zu anderen Zwecken zu verwenden (Kriminalitätsbekämpfung, Terrorabwehr usw.). Diese muss – wenn nicht bereits durch technische und konzeptionelle Maßnahmen möglich – durch unabhängige Kontrollinstanzen organisatorisch abgesichert werden (Auditrecht durch unabhängige Sachverständige bzw. eine Ethikrat). Bei einem internationalen Einsatz ist darauf zu achten, dass es wegen unterschiedlicher Rechtssysteme oder -auslegungen nicht zu einer Unterwanderung und Aufweichung des angestrebten Schutzniveaus kommt.

Ohnehin müssen der oder die Serverbetreiber zuverlässig und vertrauensvoll sein. Die Hersteller Apple und Google müssen ggf. mitwirken, was wiederum im Gegensatz zu vorheriger Maxime stehen könnte.

4.5.7 Anforderungen an Skalierbarkeit und Performance

Das Serversystem muss skalierbar und im Gutfall auf massenhafte Anfragen (aus aller Welt) gerüstet sein (Betrieb in verteilten Rechenzentren). Die Betriebskosten werden erheblich sein.

5 Konkrete Umsetzungsideen

Aus den Vorüberlegungen und den anschließenden Diskussionen im Projektteam ergeben sich verschiedene Umsetzungsideen, die es in Bezug auf deren technische Umsetzbarkeit und den Grad der Anonymisierung und Einhaltung der Datenschutzrichtlinien zu bewerten gilt.

5.1 Umsetzungsidee 1 – Plain UUID

Die Idee basiert auf der Aussendung der Standard Bluetooth UUIDs der Smartphones als Broadcast im Advertising-Modus und dem Scannen und Einsammeln dieser Informationen durch die Kontaktpartner in der näheren Umgebung und ist bereits in Kapitel 4 detailliert beschrieben. Die Smartphones der Personen A, B und C begegnen sich innerhalb der Distanz und für die Dauer, die als kritisch für die Übertragung von Infektionen angesehen wird:

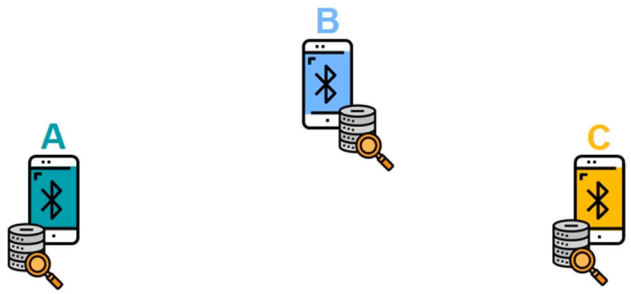

Abbildung 8: Zustand 0 - Kontaktpartner treffen aufeinander

Die Smartphones übertragen öffentlich ihre UUID:

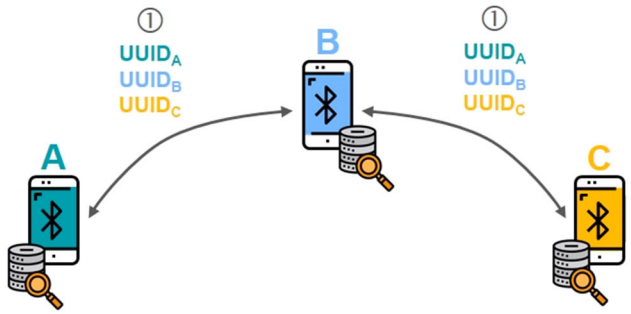

Abbildung 9: Zustand 1 - Kontaktpartner senden UUID via BLE aus

Die Apps auf den Smartphones der Personen A, B und C speichern jeweils die UUID der beiden Kontakte. Das Smartphone von A speichert also die UUIDs von B und C usw. Die Datensätze werden dabei nur lokal auf den Smartphones innerhalb der App abgelegt und mir einem Zeitstempel (tagesgenau) sowie ggf. einer bewusst verrauschten Geo-Information versehen (siehe Kapitel 4.1.2).

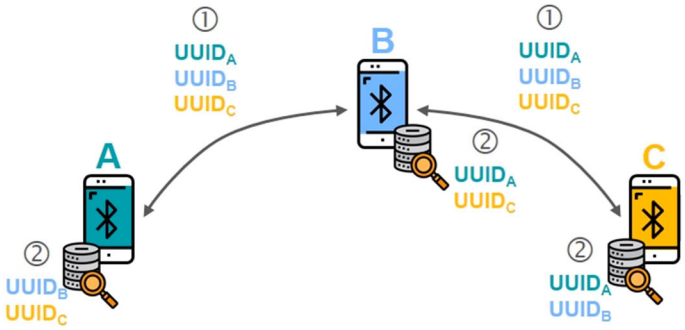

Abbildung 10: Zustand 2 - Kontaktpartner speichern UUID der anderen lokal ab

Person B wird positiv auf das „Corona“-Virus getestet und überträgt anschließend die Information über die Infektion an die zentrale Stelle (z.B. pro Land).

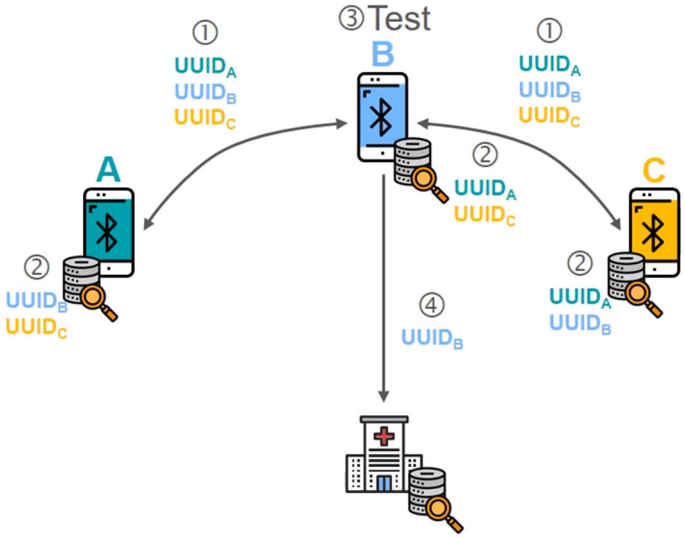

Abbildung 11: Zustand 3 und 4 - B lässt sich testen und überträgt seine UUID an Server

Auf dem Server der zentralen Stelle wird die UUID mit dem Zeitstempel der Infektion gespeichert.

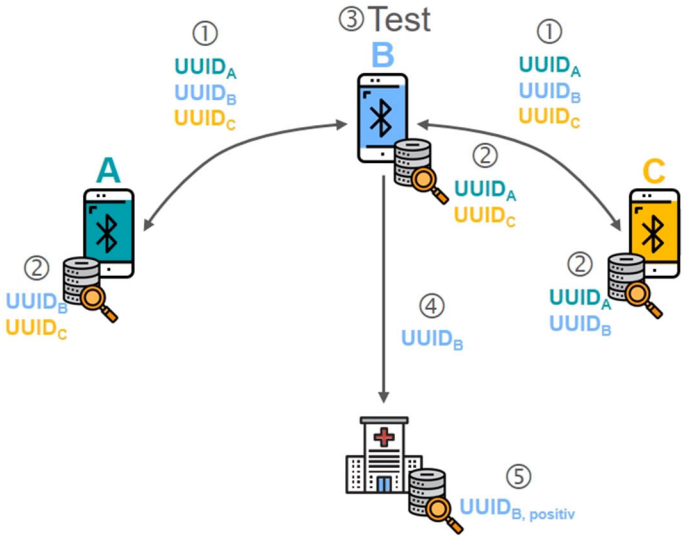

Abbildung 12: Zustand 5 - Positives Testergebnis wird zu UUID zentral hinterlegt

Person A möchte prüfen, ob in der relevanten Zeit Kontakte zu infizierten Personen stattgefunden haben. Dazu sendet das Smartphone von Person A die lokal gespeicherten UUIDs aus dem relevanten Zeitraum an die zentrale Stelle zur Überprüfung.

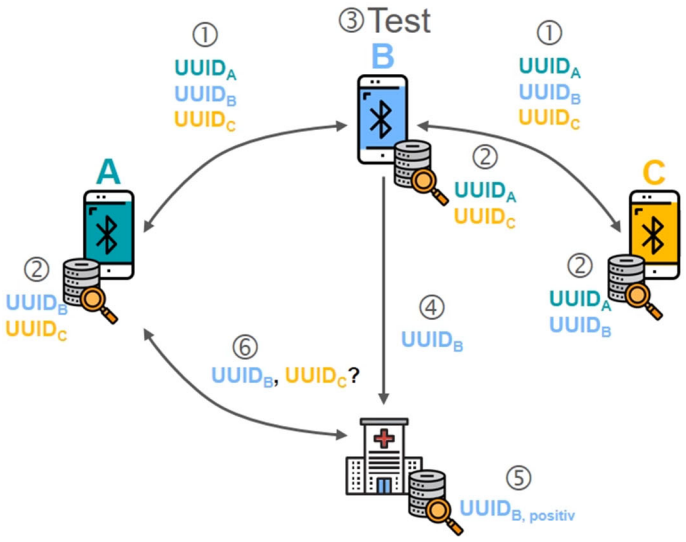

Abbildung 13: Zustand 6 - A fragt Status seiner früheren Kontakte ab

Die zentrale Stelle prüft in der zentralen Datenbank, ob die von Person A übermittelten UUIDs für den relevanten Zeitraum gelistet sind. Falls diese Prüfung positiv ist, meldet die zentrale Stelle ein erhöhtes Infektionsrisiko an Person A zurück.

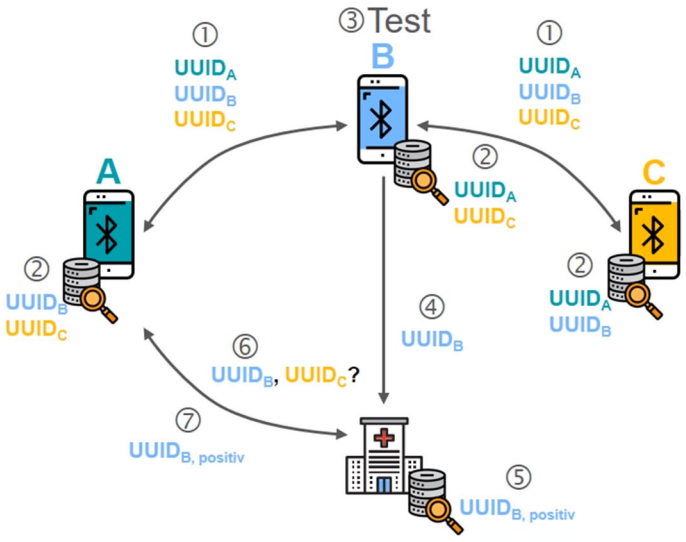

Abbildung 14: Zustand 7 - Positives Ergebnis von B wird an A übermittelt

5.1.1 Probleme

Die UUID des Smartphone ist leider in der Praxis nicht so anonymisiert und losgelöst von einer natürlichen Person, wie es in diesem Kontext wünschenswert ist. Auch wenn es zunächst keine direkte Rückschlussmöglichkeit von einer UUID auf eine Person gibt, kann diese ggf. aber durch Zusatzinformationen oder ein lokales Beobachten des Umfelds beim Scannen hinzuaggregiert werden. Gelangt man nachträglich zu einer Zuordnung von UUID zum Nutzer, werden die gesamte Kommunikation bzw. Historie enttarnt.

5.1.2 Vorteile

- Einfache technische Umsetzung.
- Erfüllt die Forderung aus dem Abstract nach der statistischen Gesamtbetrachtung.

5.1.3 Nachteile

- Im direkten Kontakt ist u.U. eine Zuordnung von UUID zu Smartphone zu Person möglich und damit auch eine Zuordnung von UUID zu Person.
- Teilnehmer kennen die UUID infizierter Personen im Klartext, können also mit Hilfe weiterer Tools bzw. Zusatzinformationen u.U. herausfinden, welche natürliche Person dazu gehört.
- Es erfolgt keine Authentifizierung der Smartphones bei der Abfrage des Gesundheitszustands von anderen UUIDs.
- Eine Abfrage von beliebigen UUIDs ist möglich.

5.1.4 Bewertung

Diese Lösung ist aus Sicht des Datenschutzes problematisch, da eine direkte Zuordnung von Personen zu UUIDs möglich und mit etwas technischem Aufwand herzustellen ist.

5.2 Umsetzungsidee 2 – Hashed UUID

Die Umsetzungsidee Hashed UUID versucht, das Problem der Speicherung der Klartext-UUIDs zu minimieren und bildet daher Hash-Werte über die eigene bzw. die erkannten UUIDs.

Die Smartphones der Personen A, B und C begegnen sich innerhalb der Distanz und für die Dauer, die als kritisch für die Übertragung von Infektionen angesehen wird:

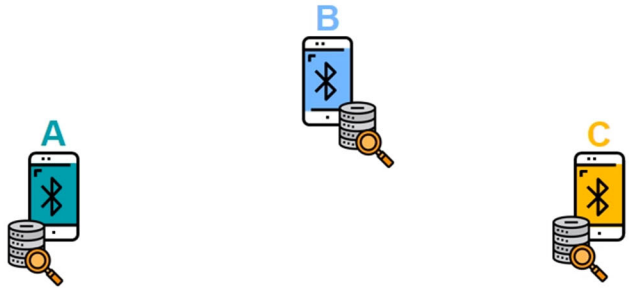

Abbildung 15: Zustand 0 - Kontaktpartner treffen aufeinander

Die Smartphones übertragen öffentlich ihre UUID:

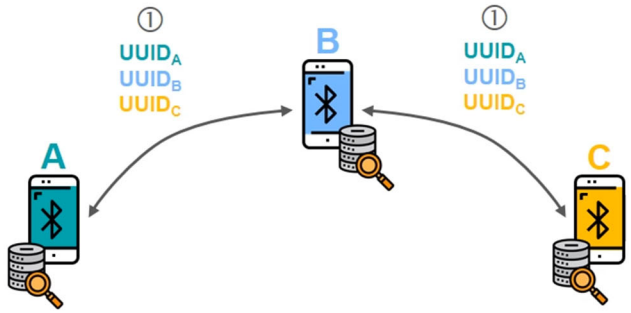

Abbildung 16: Zustand 1 - Kontaktpartner senden UUID via BLE aus

Die Apps auf den Smartphones der Personen A, B und C speichern jeweils die Hashwerte der UUID der beiden Kontakte, kombiniert mit der eigenen UUID. Das Smartphone von A speichert also Hash-Werte der UUIDs von A kombiniert mit B sowie A kombiniert mit C usw. Dabei werden die UUID vor der Hash-Wert-Bildung sortiert, so dass für einen Kontakt zwischen A und B auf beiden Smartphones der gleiche Hash-Wert ermittelt wird. Die Datensätze werden dabei nur lokal auf den Smartphones innerhalb der App abgelegt und mir einem Zeitstempel (tagesgenau) zzgl. ggf. eines verrauschten Geo-Tags versehen.

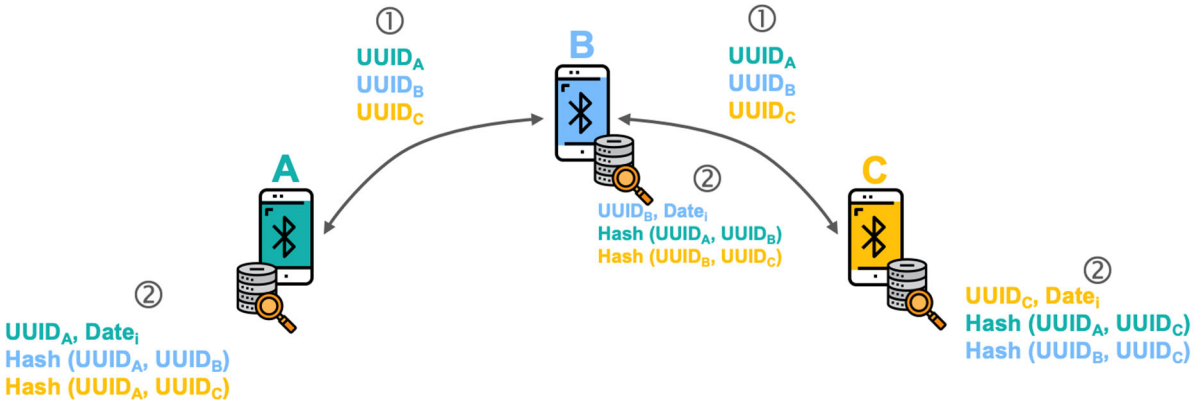

Abbildung 17: Zustand 2 - Kontaktpartner speichern hashed UUID der anderen lokal ab

Person B wird positiv auf den Corona-Virus getestet und überträgt anschließend die Information über die Infektion an die zentrale Stelle (z.B. pro Land). In dieser Information enthalten sind die eigene UUID, der Zeitstempel (tagesgenau), sowie die Hashwerte der kombinierten UUIDs von Person B mit den jeweiligen Kontaktpersonen (also Hash(UUIDA, UUIDB) sowie Hash(UUIDB, UUIDC)).

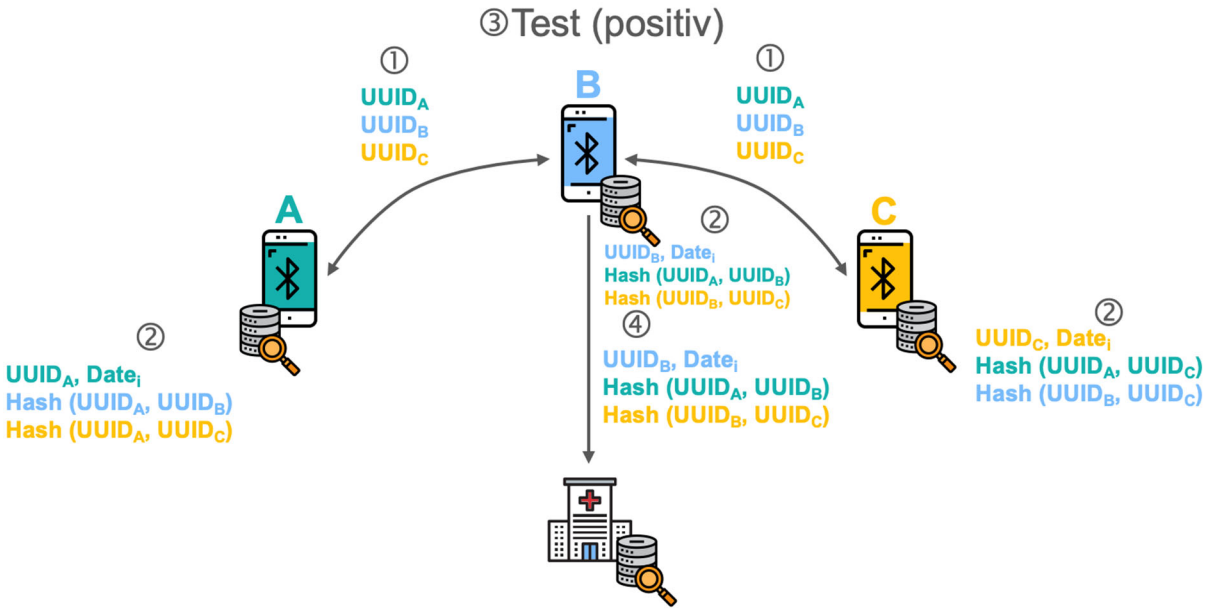

Abbildung 18: Zustand 3 und 4 - B lässt sich testen und überträgt seine UUID an Server

Auf dem Server der zentralen Stelle werden diese Informationen mit dem Zeitstempel der Infektion gespeichert.

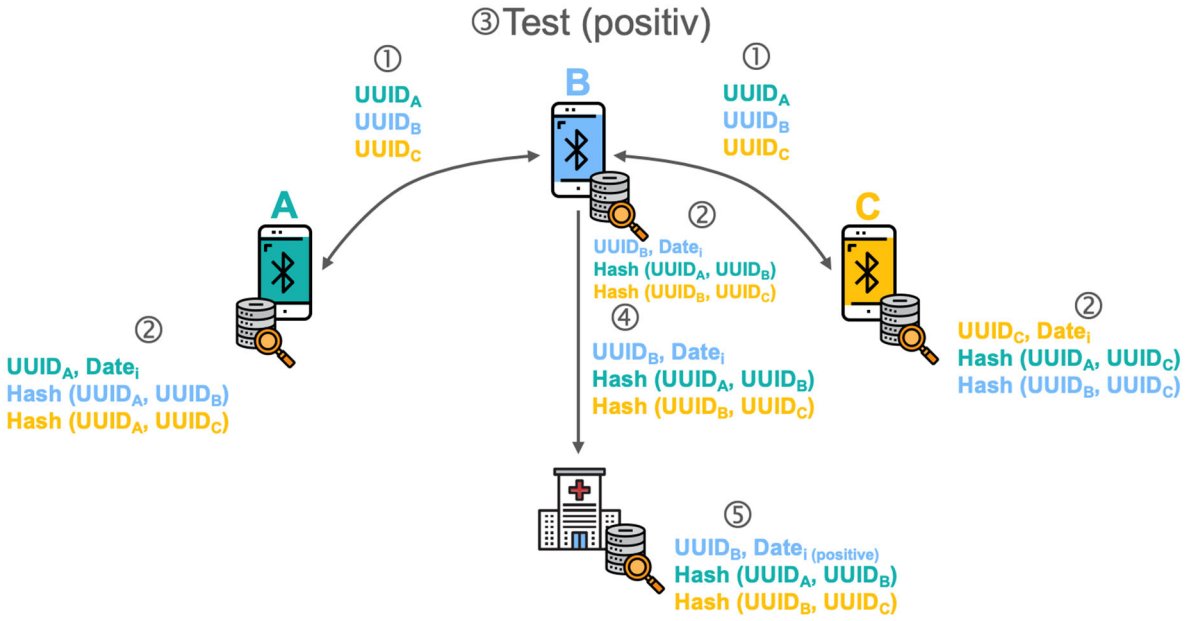

Abbildung 19: Zustand 5 - Positives Testergebnis wird zu UUID zentral hinterlegt

Person A möchte prüfen, ob in der relevanten Zeit Kontakte zu infizierten Personen stattgefunden haben. Dazu sendet das Smartphone von Person A die lokal gespeicherten Hash-Werte der eigenen Kontakte UUIDs aus dem relevanten Zeitraum an die zentrale Stelle zur Überprüfung (also Hash(UUIDA, UUIDB) sowie Hash(UUIDA, UUIDC)).

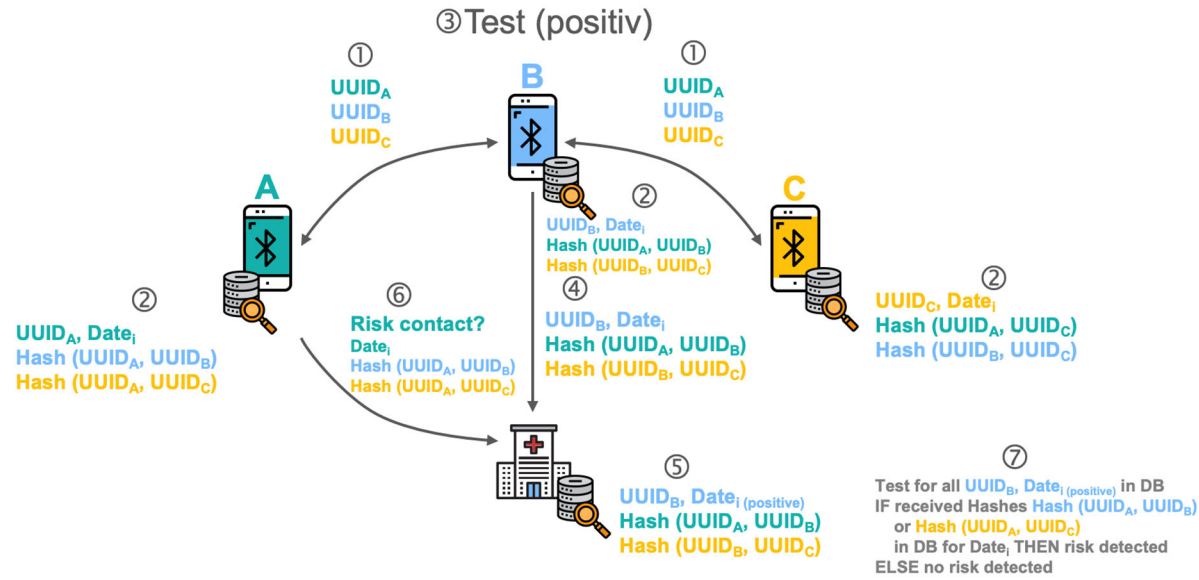

Abbildung 20: Zustand 6 und 7 - A fragt Status seiner früheren Kontakte ab

Die zentrale Stelle prüft in der zentralen Datenbank, ob die von Person A übermittelten UUIDs für den relevanten Zeitraum gelistet sind. Falls diese Prüfung positiv ist, meldet die zentrale Stelle ein erhöhtes Infektionsrisiko an Person A zurück.

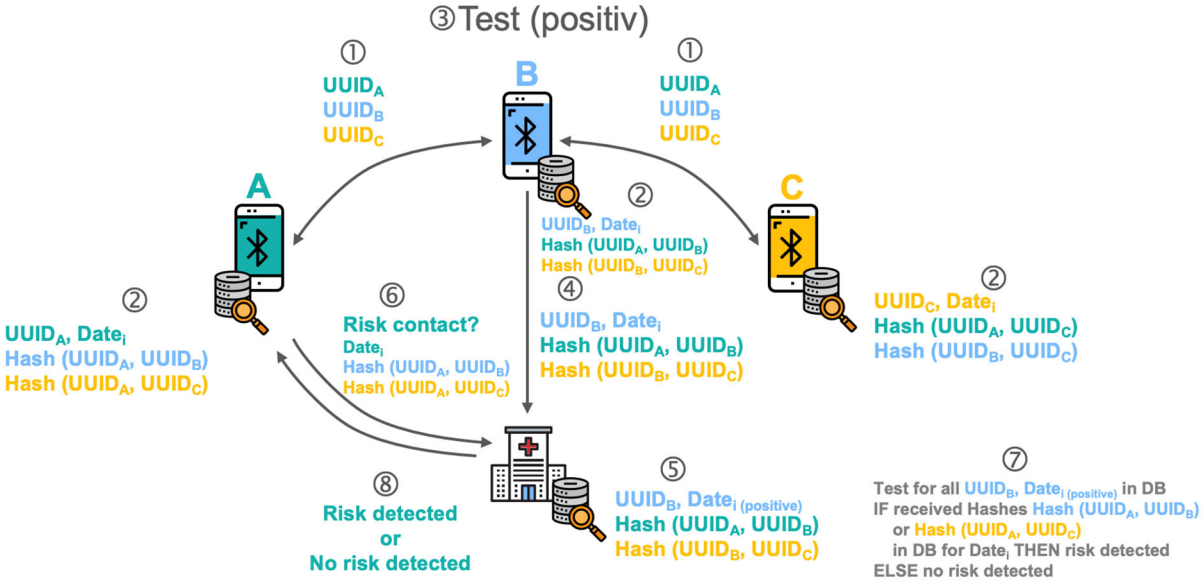

Abbildung 21: Zustand 8 - Erhöhtes Infektionsrisiko wird an A übermittelt

5.2.1 Probleme

./.

5.2.2 Vorteile

- Einfache technische Umsetzung
- Erfüllt die Forderung aus dem Abstract nach der statistischen Gesamtbetrachtung.
- Keine Zuordnung von UUID zu Smartphone zu Person möglich, da UUID nicht im Klartext vorliegt. Teilnehmer können also nur mit erheblichem technischem Aufwand herausfinden, welche natürliche Person zu einer UUID gehört.

5.2.3 Nachteile

- Es erfolgt keine Authentifizierung der Smartphones bei der Abfrage des Gesundheitszustands von anderen UUIDs.
- Eine Abfrage von beliebigen UUIDs ist möglich.

5.2.4 Bewertung

Diese Lösung ist aus Sicht des Datenschutzes deutlich besser, da eine direkte Zuordnung von Personen zu UUIDs nur mit erheblichem technischem Aufwand herzustellen ist. Auch diese Lösung erlaubt allerdings das Abfragen des Gesundheitszustands von UUIDs (und damit von Personen), mit denen überhaupt kein Kontakt stattgefunden hat.

5.3 Umsetzungsidee 3 – Random & UUID

Die 3. Umsetzungsidee Random plus UUIDs verbessert ebenso wie die Umsetzungsidee in Kapitel 5.2 die Vertraulichkeit der UUIDs, die nicht mehr auf den empfangenden Geräten gespeichert werden, und speichert weitere Informationen zum Kontakt, z.B. das Datum der Begegnung. Die Möglichkeit, Informationen über andere Benutzer anzufragen wird ausgeschlossen, allerdings zu dem Preis der Aufgabe der eigenen Anonymität im Abfragefall.

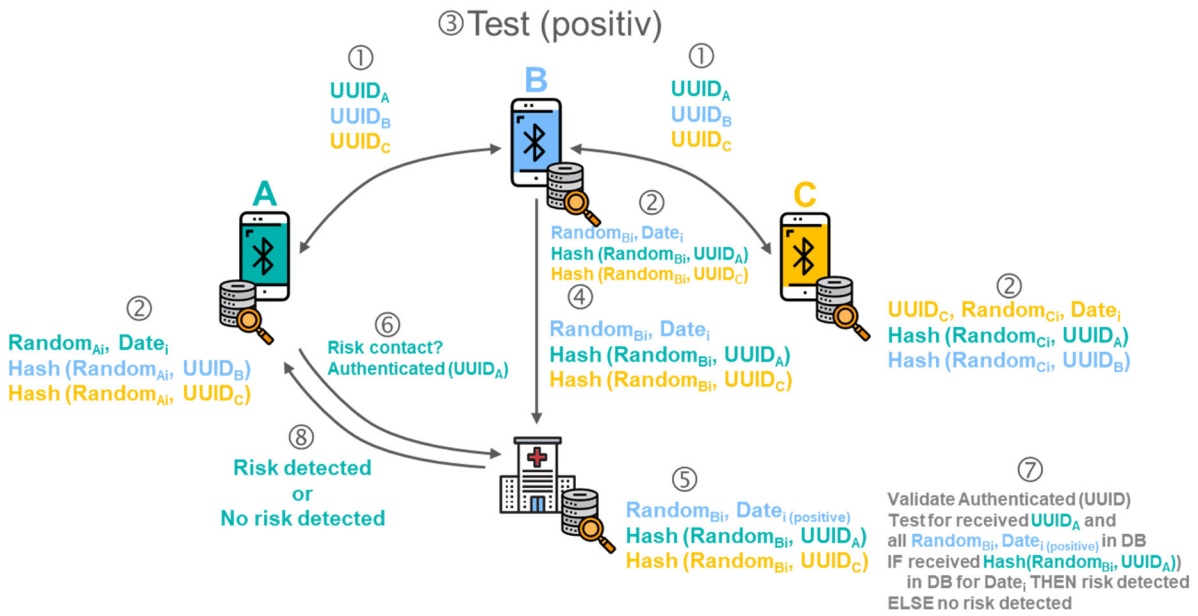

Abbildung 22: Architektur u. Austausch von Informationen zwischen den Teilnehmern – UUID

5.3.1 Vorbedingungen

- Alle Teilnehmer A, B und C haben die entsprechende App installiert, welche tageweise und anonymisiert Daten über Kontakte zu anderen Teilnehmern speichert.
- Jeder Teilnehmer X besitzt eine **$UUID_x$**. Zusätzlich generiert jeder Teilnehmer X für jeden Tag i einen teilnehmerspezifischen Zufallswert **$Random_{xi}$**, einen Datumswert **$Date_i$** und ggf. weiteren Informationen (LandesID o.ä).
- Eine zentrale Stelle (symbolisiert durch ein Krankenhaus) dient als Aufnahmestelle für die anonymisierten Kontaktlisten infizierter Personen sowie als Kontaktstelle für Personen, die unter Preisgabe ihrer UUID anfragen wollen, ob sie in der Nähe infizierter Personen gewesen sind.

5.3.2 Ablauf

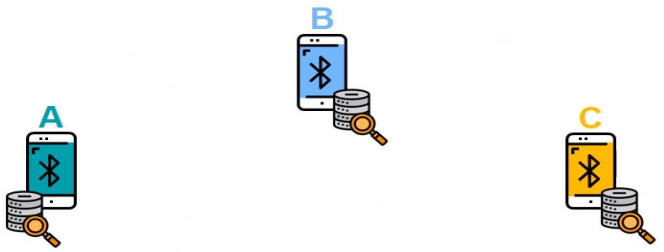

Abbildung 23: Zustand 0 - Kontaktpartner treffen aufeinander

1. Die App eines Teilnehmers generiert an einem neuen Tag i den Wert $Date_i$, einen Zufallswert **$Random_{xi}$** und speichert diese zusammen ab. Danach sendet die App periodisch die eigene $UUID_x$ per Broadcast an ihre Umgebung und sammelt parallel dazu aus der Umgebung die Identifier anderer Apps auf. Im Beispiel broadcasten die Teilnehmer ihre jeweiligen Identifier **$UUID_A$**, **$UUID_B$** und **$UUID_C$** und hören die der anderen mit.

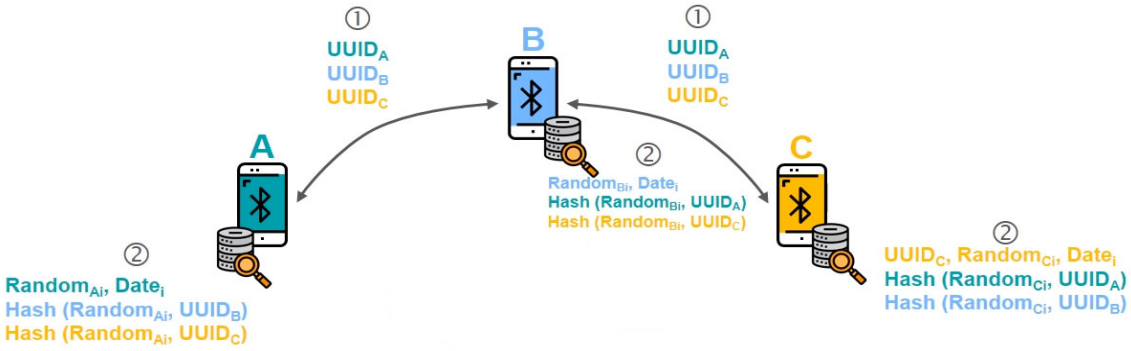

Abbildung 24: Zustand 1 und 2 - Generierung eines Random-Wertes

2. Die empfangenen UUIDs werden nicht im Klartetxt gespeichert, sondern zusammen mit der eigenen $Random_{xi}$ gehasht und gespeichert. Im Beispiel speichert Teilnehmer **A** die Einträge **Hash ($Random_{Ai}$, $UUID_B$)** und **Hash ($Random_{Ai}$, $UUID_C$)** als Indikator, dass **A** und **B** bzw. **A** und **C** in Kontakt waren. Dieser Kontakt kann im Nachgang nur nachgewiesen werden (Abgleich des Hash-Wertes), wenn die Random und UUID beider Teilnehmer erneut gemeinsam vorliegen.
3. Im Beispiel wird Teilnehmer **B** positiv auf COVID-19 getestet.

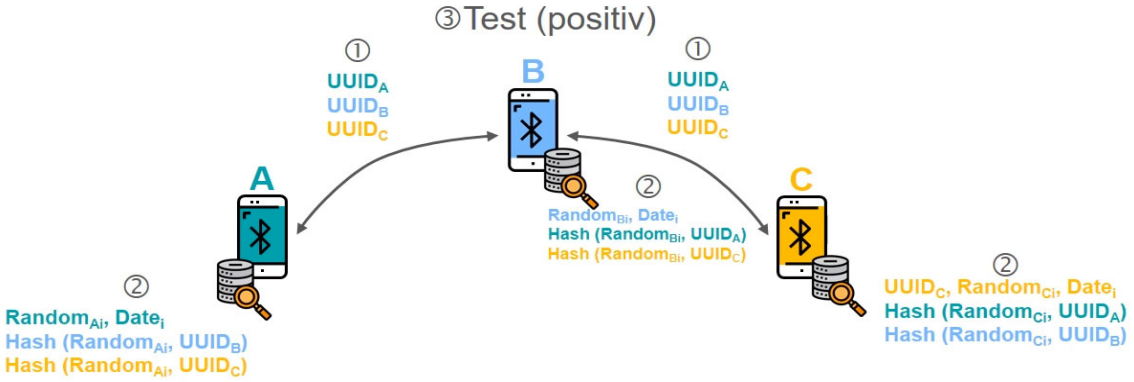

Abbildung 25: Zustand 3 - Teilnehmer B wird positiv auf Covid-19 getestet

4. Teilnehmer **B** willigt ein, dass seine Daten zur Kontaktermittlung verwendet werden dürfen. Dazu überträgt **B** die lokal gespeicherte und im Zeitfenster liegenden Werte **Random$_{Bi}$**, **Date$_i$** zusammen mit den dazu anonymisiert gespeicherten Teilnehmerkontakten in verschlüsselter Form an die zentrale Stelle. Hierbei ist sicherzustellen, dass die Informationen tatsächlich von **B** kommen, was hier nicht weiter beschrieben wird.

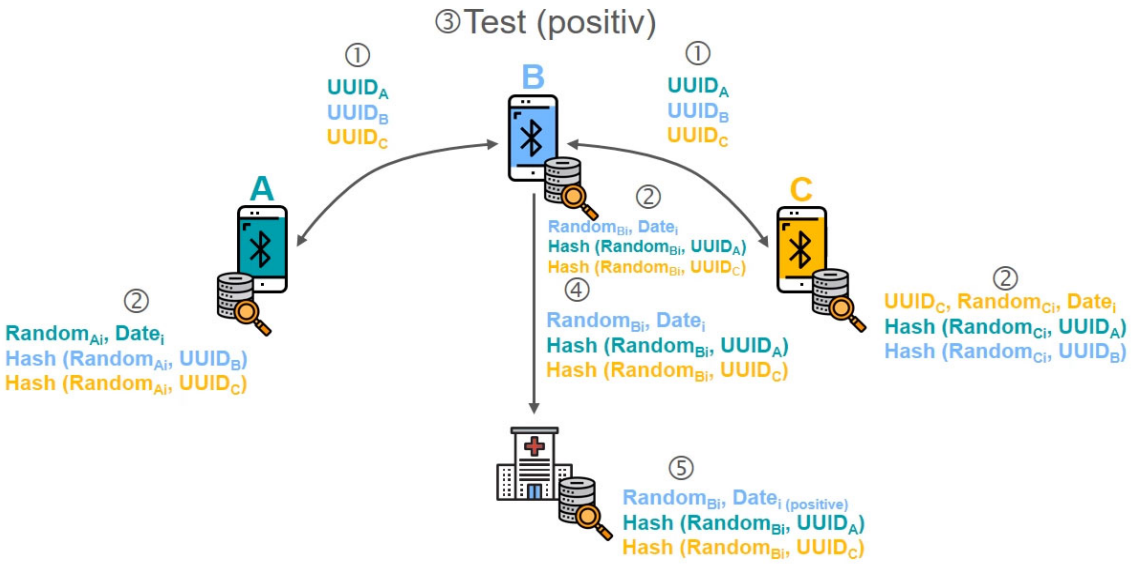

Abbildung 26: Zustand 4 und 5 - Teilnehmer B willigt in Übertragung und Speicherung ein

5. Die zentrale Stelle nimmt die Daten entgegen, kennzeichnet die Daten von **B** als die eines Infizierten und speichert u.a. die mit dem Tag i verbundenen Daten **Random$_{Bi}$**, **Date$_i$**, **Hash (Random$_{Ai}$, UUID$_B$)** und **Hash (Random$_{Bi}$, UUID$_C$)**. Man beachte, dass die zentrale Stelle nun zwar **B** kennt, nicht jedoch **A** oder **C**. Die Kontakt-Hashwerte sind also (noch) nicht nutzbar.

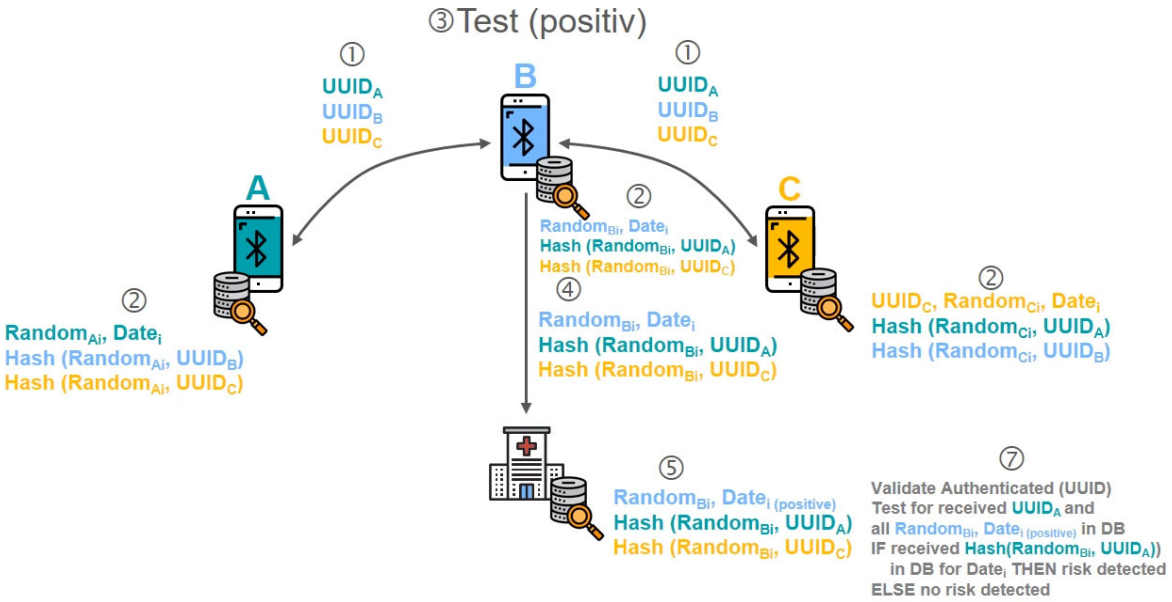

Abbildung 27: Zustand 7 - Verarbeitung beim Server

6. Teilnehmer **A** entscheidet sich, seine Kontakthistorie auf mögliche Kontakte mit Infizierten prüfen zu lassen. Dazu gibt er seine **$UUID_A$** preis, indem er sie in authentifizierter Form (**Authenticated ($UUID_A$)**) und in sicherer Form an die zentrale Stelle sendet.

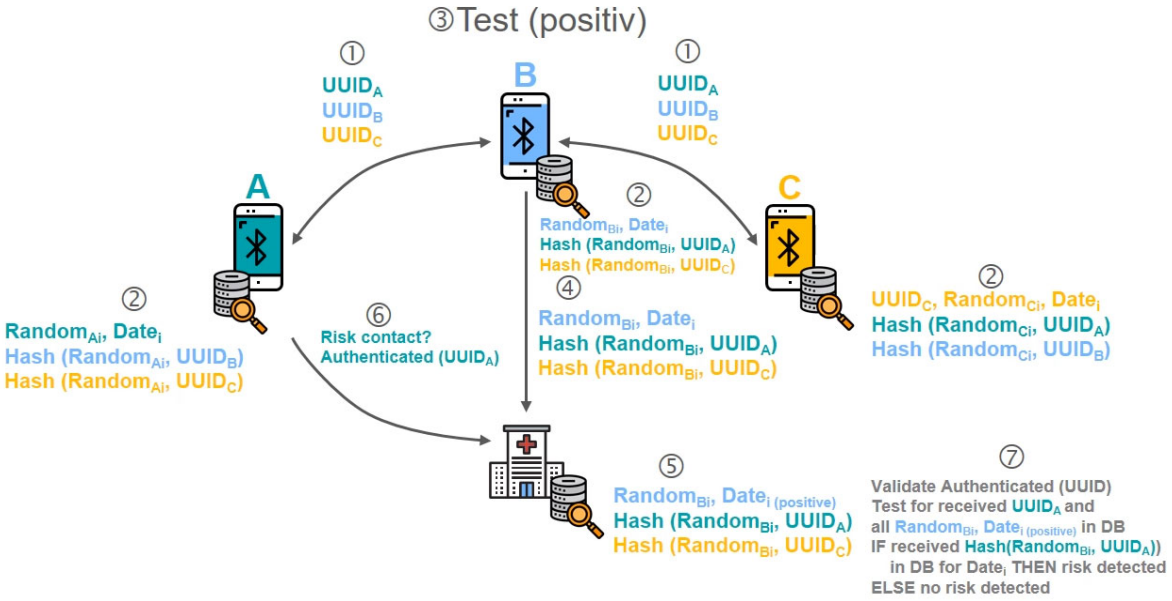

Abbildung 28: Zustand 6 - Teilnehmer A fragt Zustand seiner Kontakte ab

7. Die zentrale Stelle hat nun die Möglichkeit, Kontakte zu infizierten Personen zu prüfen. Dazu generiert die zentrale Stelle für das relevante Zeitfenster die empfangenen UUID-Werte mittels den Zufallswerten der Infizierten und der verwendeten Hash-Funktion entsprechende Hash-Werte.

Im Beispiel generiert die zentrale Stelle mit dem von A gesendeten **$UUID_A$** u.a. den Hash-Wert **Hash ($Random_{Ai}$, $UUID_B$)** und kann somit den Kontakt zu einem Infizierten nachweisen. Wäre der Hash-Wert nicht in der Liste für Tag i gespeichert, wurde von **B** kein Kontakt registriert.

8. Das Ergebnis des Abgleichs wird Teilnehmer **A** verschlüsselt mitgeteilt. Teilnehmer **A** steht es nun frei, unter Vorlage des Kontaktnachweises weitere Schritte zu unternehmen.

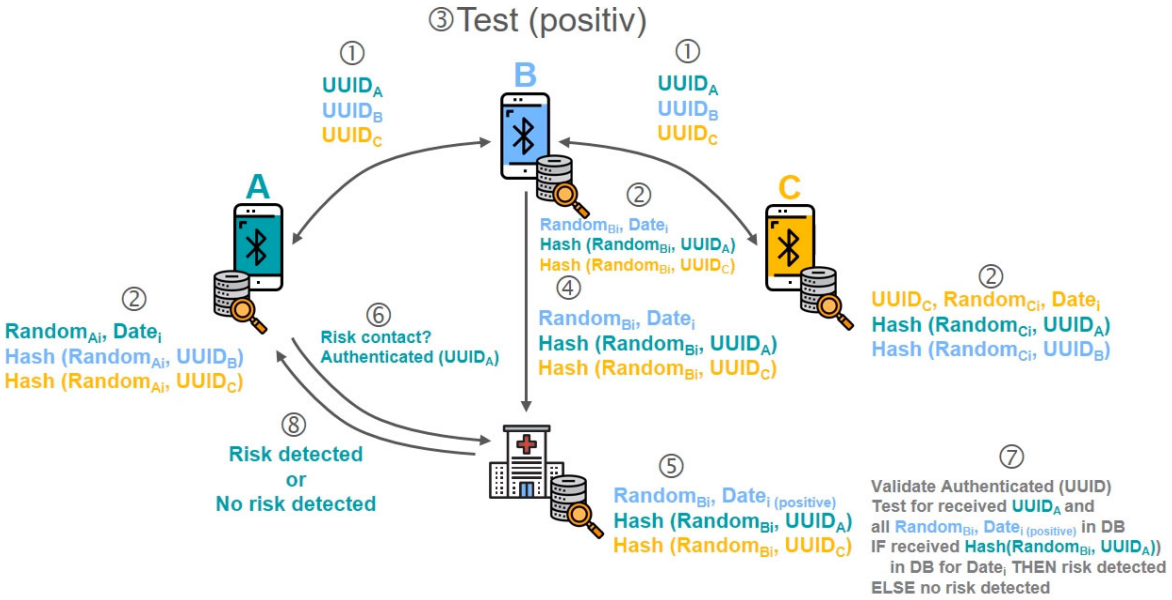

Abbildung 29: Zustand 8 - Rückmeldung des Ergebnisses an Teilnehmer A

5.3.3 Probleme

./.

5.3.4 Vorteile

- Der Vorteil der Lösung ist, dass kein Angreifer eine Anfrage an das System stellen kann, die nicht von ihm selbst kommt. Auch werden keine UUIDs anderer Telefone gespeichert.

5.3.5 Nachteile

- Der Anfragende gibt spätestens bei Schritt 6 seine volle Anonymität auf, da er seine UUID angeben muss

5.3.6 Bewertung

Diese Lösung verzichtet auf das lokale Speichern eingesammelter UUIDs und verhindert ein willkürliches Abfragen beliebiger Daten der zentralen Stelle. Erkauft wird dies jedoch durch den zu diskutierenden Nachteil, dass der Abfragende sich mit Verlust seiner vorher vollständigen Anonymität beim Server authentifiziert. Dies erfolgt jedoch nicht mit Klarnamen, sondern mit seiner UUID und daher ist der Nachteil nicht allzu hoch zu bewerten und in etwa vergleichbar mit dem in Lösung 1 „Plain UUID“ (Kapitel 5.1).

5.4 Umsetzungsidee 4 – Hashed Temporary-ID

Die 4. Umsetzungsidee Hashed Temporary basiert auf Smartphones, die mittels einer App per Bluetooth temporäre Identitäten austauschen. Im Infektionsfall kann ein Teilnehmer Infos zu seiner Identität sowie anonymisierte Kontaktereignisse mit anderen Teilnehmern an eine zentrale Stelle übertragen. Andere Teilnehmer können anonymisiert Anfragen zu dieser zentralen Kontaktstelle stellen, um festzustellen, ob sie in einem begrenzten Zeitraum der Vergangenheit Kontakt zu einem Infizierten hatten.

Sie verwendet also keine UUIDs, sondern einen wechselnden (temporären) Identifier (T-ID). Es wird nur einer pro Tag generiert und nur lokal dauerhaft gespeichert. Knoten speichern keine T-IDs anderer Geräte.

5.4.1 Vorbedingungen:

- Alle Teilnehmer A, B und C haben die entsprechende App installiert, welche tageweise und anonymisiert Daten über Kontakte zu anderen Teilnehmern speichert.
- Es gibt für jeden Teilnehmer X und jeden Tag i einen temporären Identifier **$T\text{-}ID_{Xi}$**. Dieser basiert auf dem Hash-Wert einem tages- und teilnehmerspezifischen Zufallswert **$Random_{Xi}$**, dem Datum **$Date_i$** und ggf. weiteren Informationen (LandesID o.ä). Beispielhaft berechnet sich der Identifer $T\text{-}ID_{Xi} = Hash(Random_{Xi}, Date_i)$, wobei Hash für eine sichere, kryptografische Hash-Funktion steht. Durch den Zufallswert und die Hash-Funktion wird sichergestellt, dass der Identifier eindeutig[7] und zufällig ist, d.h. ohne weitere Kontextinformationen ist eine Zuordnung zu einem Gerät bzw. Nutzer nicht möglich. Zudem ist es nicht möglich, aus dem Hash-Wert den Zufallswert oder das Datum zu berechnen. Der Datumswert sorgt dafür, dass Daten, die außerhalb eines rückläufigen Zeitfensters liegen, gelöscht werden können.
- Eine zentrale Stelle (symbolisiert durch ein Krankenhaus) dient als Aufnahmestelle für die anonymisierten Kontaktlisten infizierter Personen sowie als Kontaktstelle für Personen, die anonym anfragen wollen, ob sie in der Nähe infizierter Personen gewesen sind.

5.4.2 Ablauf (Tag I)

1. Die App eines Teilnehmers generiert an einem neuen Tag i die Werte $Random_{Xi}$ und $Date_i$, bildet den Hash über diese Wert und erhält so den an diesem Tag zu benutzenden, temporären Identifier $T\text{-}ID_{Xi}$. Alle drei Werte werden lokal gespeichert (Teilnehmer **A** speichert z.B. **$T\text{-}ID_{Ai}$, $Random_{Ai}$, $Date_i$**). Danach sendet die App periodisch die eigene $T\text{-}ID_{Xi}$ per Broadcast an ihre Umgebung und sammelt parallel dazu aus der Umgebung die Identifier anderer Apps auf. Im Beispiel broadcasten die Teilnehmer ihre jeweiligen Identifier **$T\text{-}ID_{Ai}$**, **$T\text{-}ID_{Bi}$** und **$T\text{-}ID_{Ci}$** und hören die der anderen mit.

[7] Abgesehen von bei Pseudozufallszahlen und kryptografischen Hashfunktionen extrem selten vorkommenden Kollisionen.

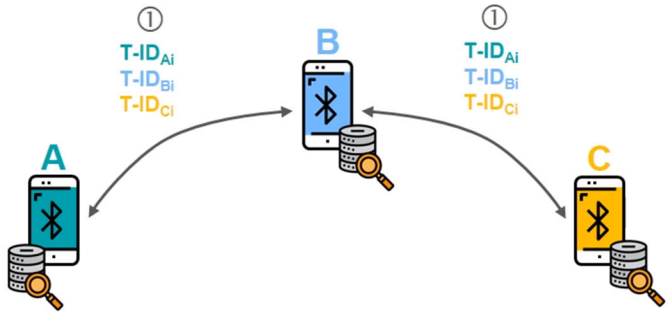

Abbildung 30: Zustand 1 - Generierung temporärere IDs

2. Die empfangenen Identifier werden nicht gespeichert, sondern zusammen mit dem eigenen Identifier konkateniert, gehasht und dieser Hash wird gespeichert. Im Beispiel speichert Teilnehmer **A** die Einträge **Hash (T-IDAi, T-IDBi)** und **Hash (T-IDAi, T-IDCi)** als Indikator, dass **A** und **B** bzw. **A** und **C** in Kontakt waren. Dieser Kontakt kann im Nachgang nur nachgewiesen werden (Abgleich des Hash-Wertes), wenn die T-IDs beider Teilnehmer erneut gemeinsam vorliegen.

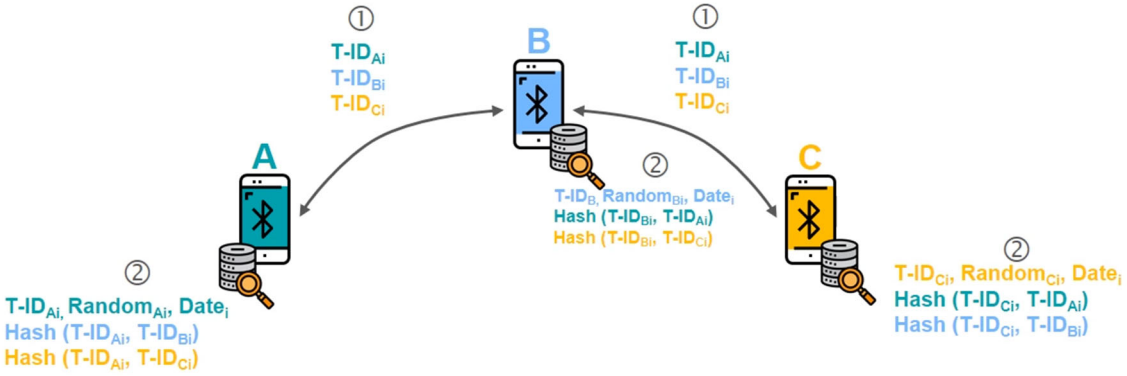

Abbildung 31: Zustand 2 - Konkatenierung der Identifier mit eigenem Identifier

3. Im Beispiel wird Teilnehmer **B** positiv auf COVID-19 getestet.

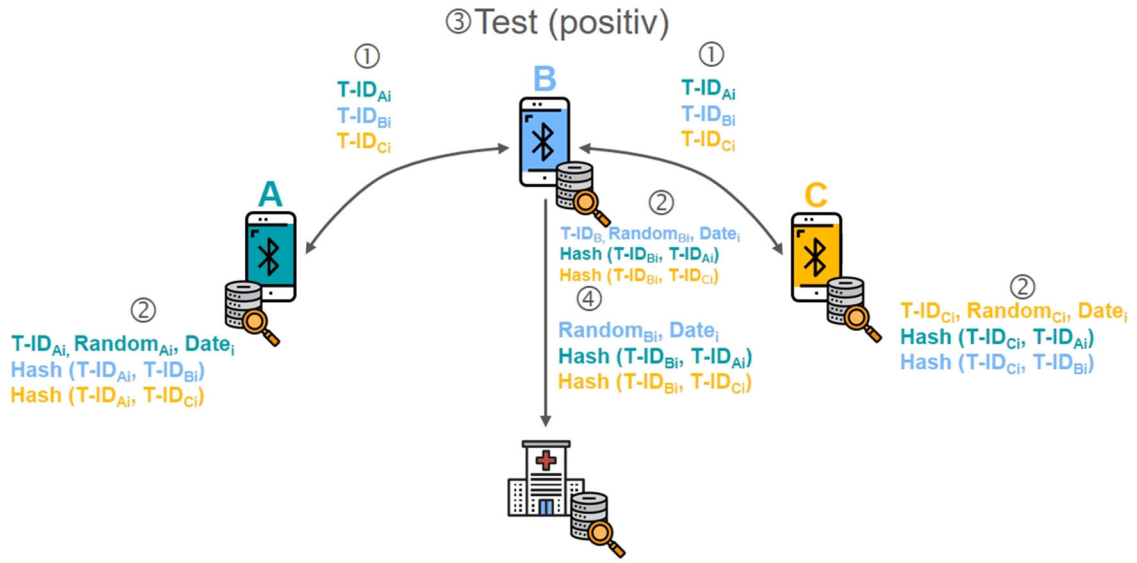

Abbildung 32: Zustand 3 und 4 - Teilnehmer wird positiv getestet

4. Teilnehmer **B** willigt ein, dass seine Daten zur Kontaktermittlung verwendet werden dürfen. Dazu überträgt **B** die lokal gespeicherte und im Zeitfenster liegenden Werte **Random$_{Bi}$**, **Date$_i$** zusammen mit den dazu anonymisiert gespeicherten Teilnehmerkontakten in verschlüsselter Form an die zentrale Stelle. Zu beachten ist, dass **T-ID$_B$** nicht versendet werden muss, da es aus den beiden anderen Werten berechnet werden kann. Dies dient zudem als Nachweis, dass ein später verwendetes **T-ID$_B$** tatsächlich von **B** stammt, da nur **B** den Wert **Random$_{Bi}$** kennen kann.

5. Die zentrale Stelle nimmt die Daten entgegen, kennzeichnet die Daten von **B** als die eines Infizierten und speichert u.a. die mit dem Tag i verbundenen Daten **Random$_{Bi}$**, **Date$_i$**, **Hash (T-ID$_{Bi}$, T-ID$_{Ai}$)** und **Hash (T-ID$_{Bi}$, T-ID$_{Ci}$)**. Man beachte, dass die zentrale Stelle nun zwar **T-ID$_{Bi}$** berechnen kann, nicht aber die zu **A** oder **C** gehörenden Identifier **T-ID$_{Ai}$** und **T-ID$_{Ci}$**. Die Kontakt-Hashwerte sind also (noch) nicht nutzbar.

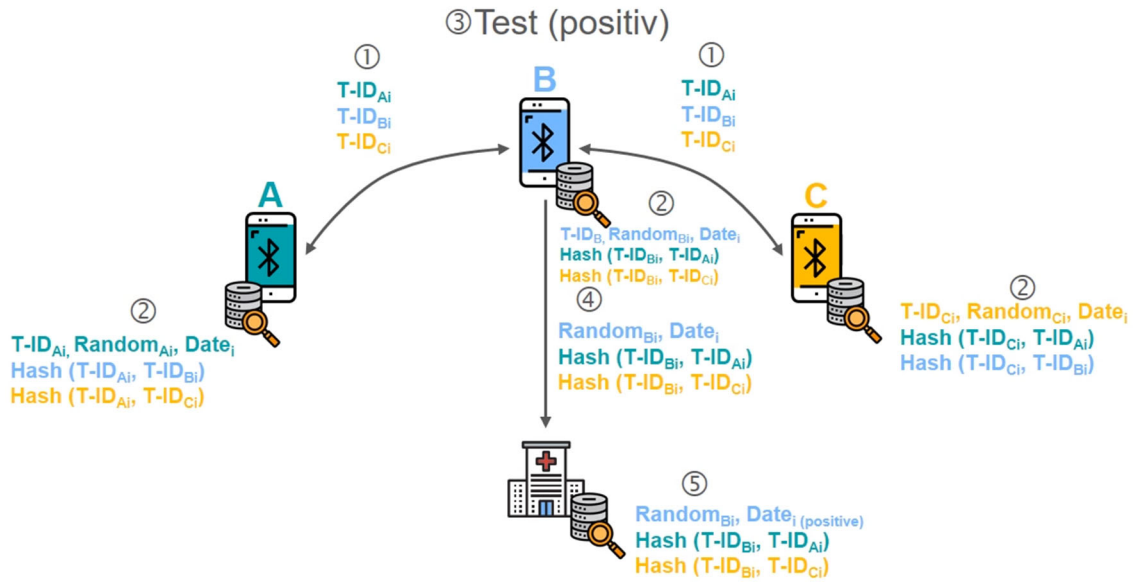

Abbildung 33: Zustand 5 - Verarbeitung durch zentrale Stelle

6. Teilnehmer **A** entscheidet sich, seine Kontakthistorie auf mögliche Kontakte mit Infizierten prüfen zu lassen. Dazu sendet er die Werte **$Random_{Ai}$** und **$Date_i$** des passenden Zeitfensters in verschlüsselter Form an die zentrale Stelle.

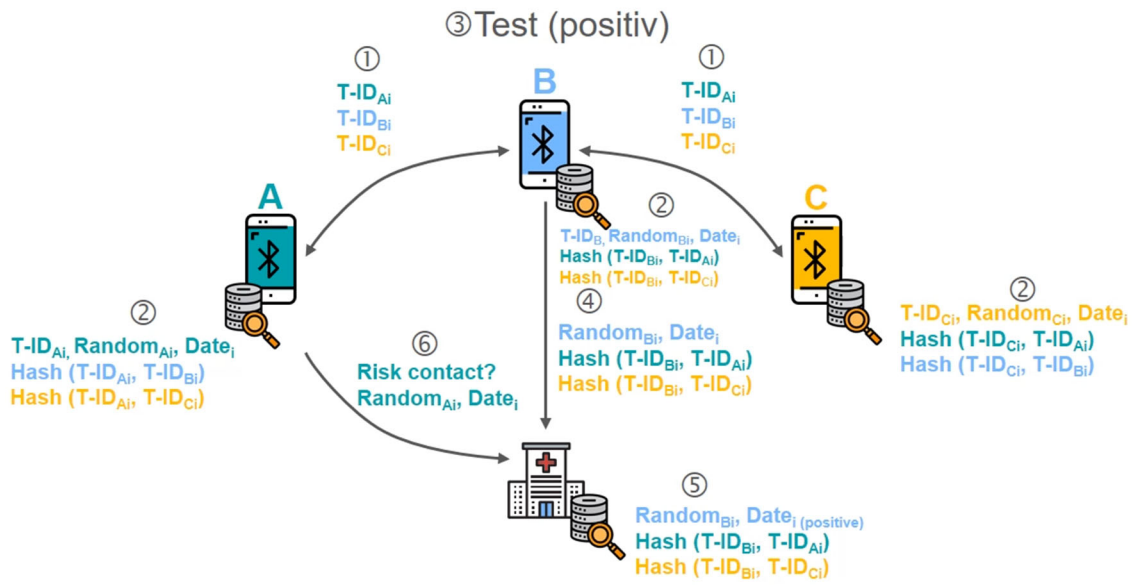

Abbildung 34: Zustand 6 - A fragt Kontakthistorie ab

7. Die zentrale Stelle hat nun die Möglichkeit, Kontakte zu infizierten Personen zu prüfen. Dazu entschlüsselt die zentrale Stelle die Werte und berechnet daraus den Identifier **$T\text{-}ID_{Ai}$ = Hash ($Random_{Ai}$, $Date_i$)**. Dies dient auch hier implizit als Nachweis, dass ein später verwendetes **$T\text{-}ID_{Ai}$** tatsächlich von **A** stammt, da nur **A** den Wert **$Random_{Ai}$** kennen kann. Im passenden Zeitfenster berechnet die zentrale Stelle für alle Infizierten deren temporären Identifier, u.a. den Wert **$T\text{-}ID_{Bi}$ = Hash ($Random_{Bi}$, $Date_i$)**. Diese Identifier werden jeweils zusammen mit dem Identifier des Anfragenden gehasht und anschließend geprüft, inwieweit die Hash-Werte für den entsprechenden Infizierten und den besagten Tag i in dessen Kontaktliste gespeichert sind. Im Beispiel berechnet die zentrale Stelle hier **Hash (Hash ($Random_{Bi}$, $Date_i$), Hash($Random_{Ai}$, $Date_i$)) = Hash ($T\text{-}ID_{Bi}$, $T\text{-}ID_{Ai}$)**. Dieser Wert findet sich tatsächlich in der Liste für Tag i der infizierten Person **B**, d.h. es kann jetzt (und wirklich erst jetzt) gefolgert werden, dass Person **A** am besagten Tag Kontakt zu **B** hatte. Wäre der Hash-Wert nicht in der Liste für Tag i gespeichert, wurde von **B** kein Kontakt registriert.

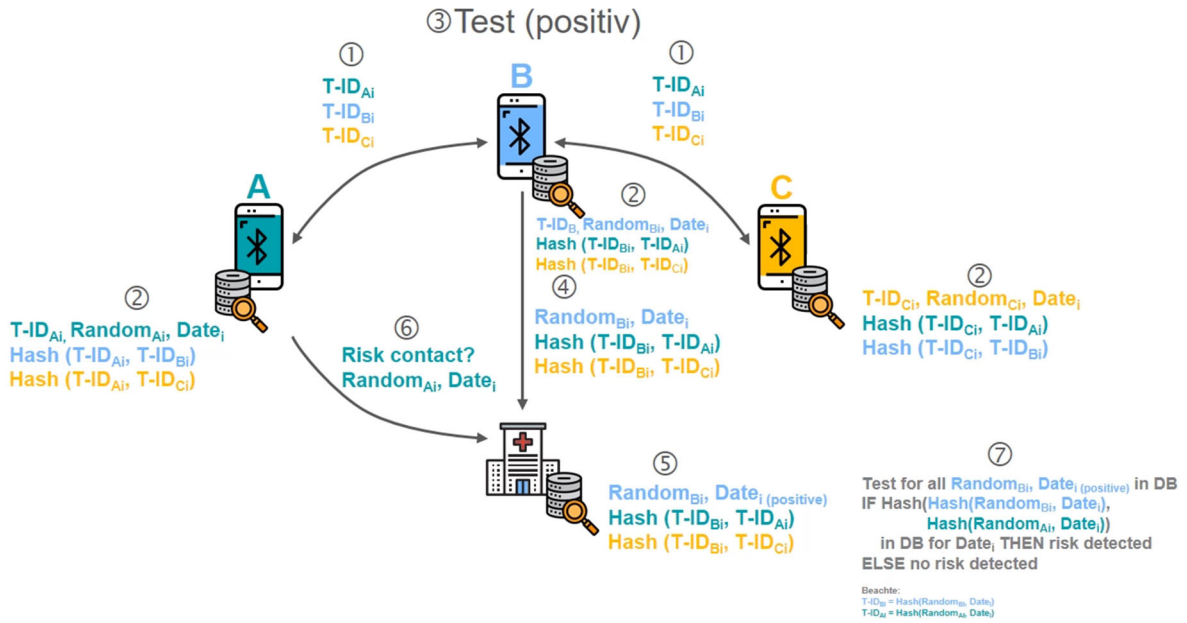

Abbildung 35: Zustand 7 - Legitimationsprüfung des Anfragenden in zentraler Stelle

8. Das Ergebnis des Abgleichs wird Teilnehmer **A** verschlüsselt mitgeteilt. Teilnehmer **A** steht es nun frei, unter Vorlage des Kontaktnachweises weitere Schritte zu unternehmen.

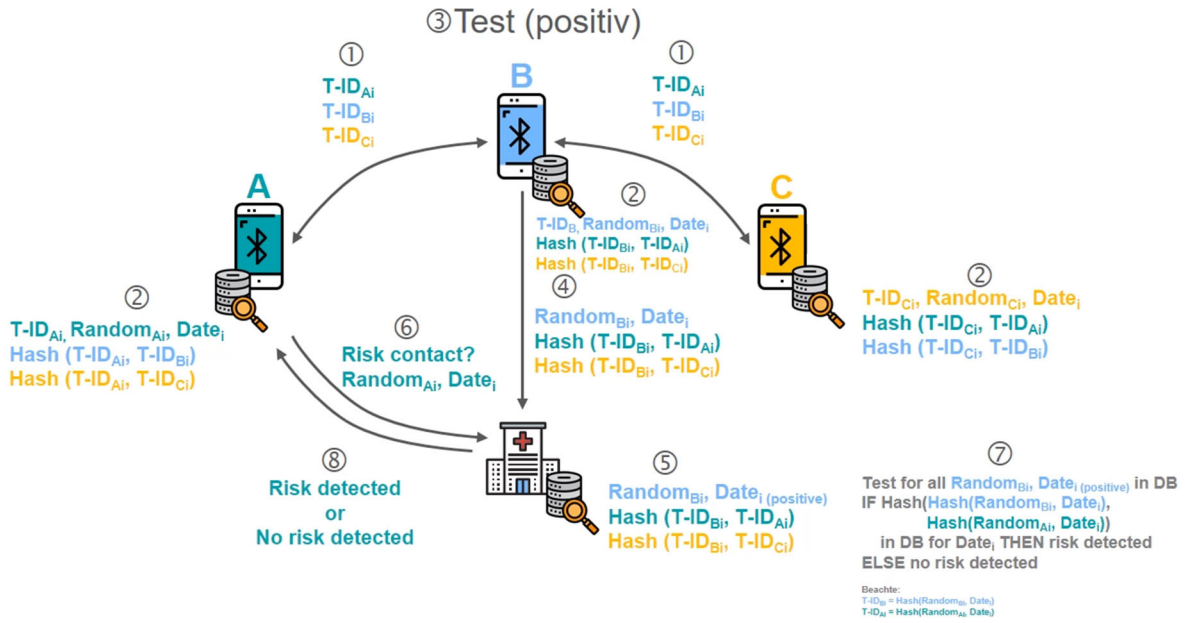

Abbildung 36: Zustand 8 - Rückmeldung des Ergebnisses der Kontakthistorie an Anfragenden A

5.4.3 Probleme

Die Autoren sind sich zum Zeitpunkt der Erstellung des Dokumentes nicht sicher, ob eine App auf den Bluetooth-Stack des Betriebssystems in einer Weise zugreifen kann, dass im Advertising bzw. Scanner-Modus zusätzliche Informationen wie die temporären Identifier ausgesendet und empfangen werden können. Die hier vorgestellte Lösung benötigt das Generieren von IDs, die explizit ohne vorheriges Pairen via Bluetooth-Advertising-Broadcast gesendet werden. Das Betriebssystem iOS von Apple, ggf. aber auch Google in Android lassen das möglicherweise nicht zu[8].

Zudem ist noch zu bewerten, ob ein böswilliger Nutzer nicht trotz anonymer Temp-ID eine direkte Beziehung zum Smartphone eines gegenüberstehenden Kontaktpartners herstellen kann. Er „sieht“ im Moment des Kontakts unweigerlich auch dessen per Bluetooth ausgesendete UUID und kann den von ihm eigentlich anonymisiert gespeicherter Kontakt später wieder einem Smartphone 1:1 via UUID zuordnen.

5.4.4 Vorteile

- Auf normalem Wege (Nutzung der offiziellen App) kein Rückschluss auf Gerät, keine Korrelation möglich
- Gezielte Angriffe durch Korrelation mit weiteren Daten zwar grundsätzlich möglich, aber nur mit erheblichem technischem Aufwand und nur für einen Tag.
- Anwender können nicht den Infektionsstand eines anderen abfragen, sondern nur den eigenen Kontakt zu solchen Infizierten[9].
- Authentifizierung über die generierte temporäre ID.
- Zentrale Stelle kann dies sowie potentiellen Kontakt zu als infiziert gemeldeten Personen prüfen. Die Prüfung ist nur möglich, wenn T-ID-Besitzer einwilligen.

5.4.5 Nachteile

- Technische Umsetzung durch erforderlichen Zugriff auf das Betriebssystem ggf. aufwändiger als andere Lösungen bzw. ist ggf. nicht möglich.

5.4.6 Bewertung

Diese Lösung ist aus Sicht des Datenschutzes die beste Lösung, da zu keiner Zeit die UUID in die Datenübertragung einfließt. Die Nutzung einer täglich wechselnden, temporären ID macht alle Arten von möglichen Angriffen auf das System deutlich schwieriger, weil die Angriffe im Prinzip jeden Tag erneut und vollständig durchgeführt werden müssten. Die temporäre ID wird hier auch zur Authentifizierung der App gegenüber der zentralen Stelle genutzt, so dass zusätzliche Zertifikate nicht unbedingt erforderlich sind.

[8] Quellen u.a. https://www.elektroniknet.de/elektronik/kommunikation/bluetooth-low-energy-in-smartphones-wie-funktioniert-das-103061-Seite-5.html und https://www.elektroniknet.de/elektronik/kommunikation/bluetooth-low-energy-in-smartphones-wie-funktioniert-das-103061-Seite-2.html

[9] Der Einfachheit halber werden hier nur positiv getestete und nicht positiv getestete unterschieden.

5.5 Umsetzungsidee 5 – Independent Application-ID

Die Umsetzungsidee mit Independent App-IDs hat das primäre Ziel, eine zentrale Auswertung von Kontakten (statistische Gesamtauswertung) zu erreichen und trotzdem eine weitestgehende Anonymität der Teilnehmer zu gewährleisten.

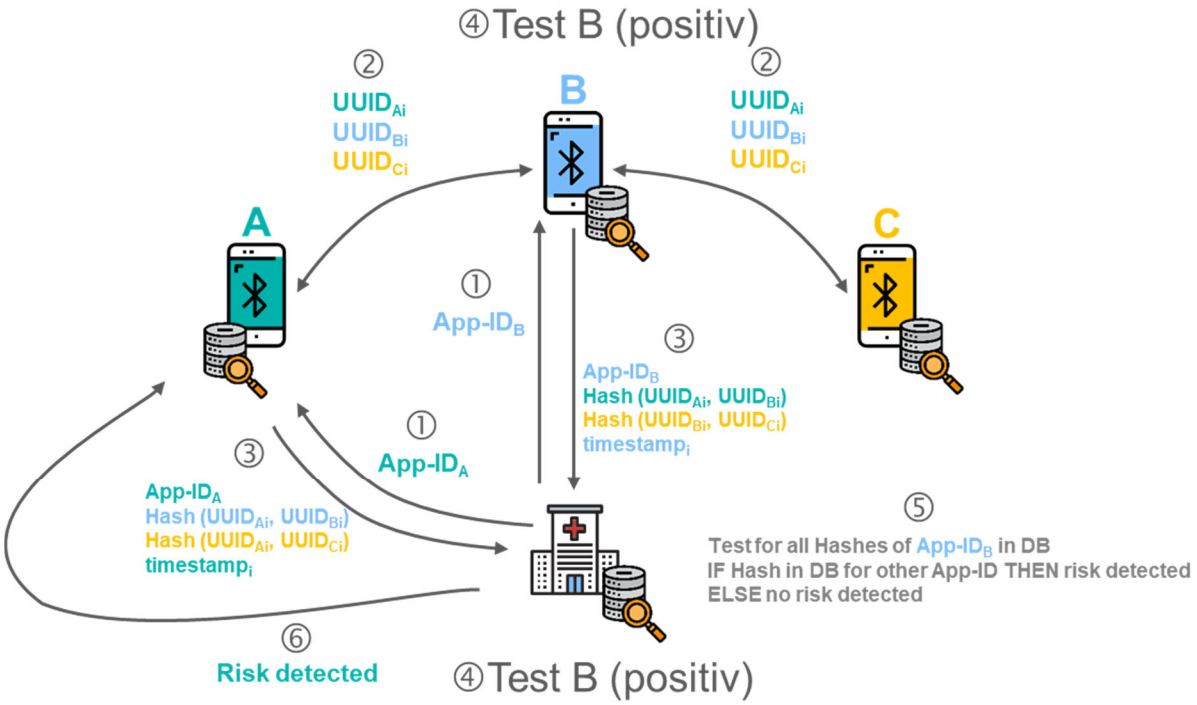

Abbildung 37: Architektur u. Austausch von Informationen zwischen den Teilnehmern – App-ID

5.5.1 Vorbedingungen

- Alle Teilnehmer A, B und C haben die entsprechende App installiert, welche anonymisiert Daten über Kontakte zu anderen Teilnehmern zwischenspeichert und diese regelmäßig gesichert an eine zentrale Stelle schickt.
- Jeder Teilnehmer X besitzt eine **$UUID_{Xi}$**, die von einem Gerät im Nahbereich öffentlich ausgesendet wird; diese besitzt eine zeitlich wechselnde Zufallskomponente i.
- Eine zentrale Stelle (symbolisiert durch ein Krankenhaus) dient als Aufnahmestelle für die anonymisierten Kontaktlisten infizierter Personen und kann empfangene Kontaktinformationen aller Teilnehmer zentral auswerten.

5.5.2 Ablauf

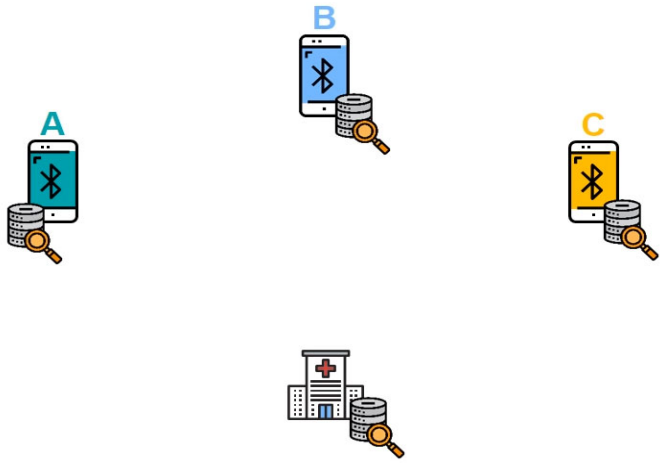

Abbildung 38: Zustand 0 - Kontaktpartner treffen aufeinander

1. Die Teilnehmer erhalten bei der Installation der App eine zufällig generierte App-ID. Die Teilnehmer **A**, **B** und **C** erhalten also die App-IDs **App-ID$_A$**, **App-ID$_B$** und **App-ID$_C$**. Die App-ID ist nur der zentralen Server-Instanz und der App selbst bekannt und dient primär zur sicheren Identifikation des Teilnehmers.

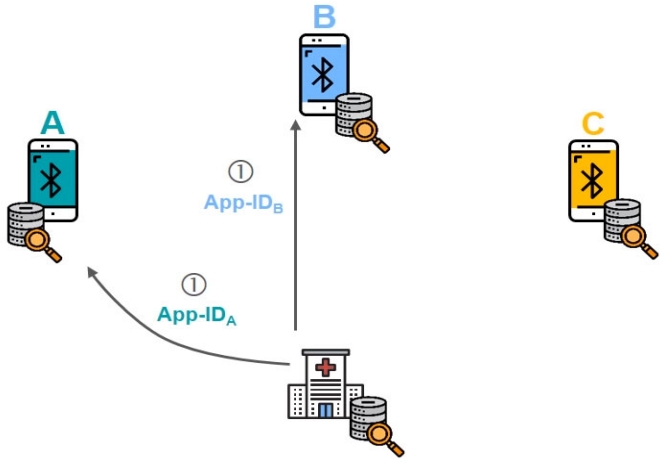

Abbildung 39: Zustand 1 - App-Nutzer erhalten bei Installation eine eindeutige App-ID

2. Jeder Teilnehmer sendet periodisch per Bluetooth die eigene UUID$_{Xi}$ per Broadcast an ihre Umgebung und sammelt parallel dazu aus der Umgebung die Identifier anderer Apps auf. Im Beispiel broadcasten die Teilnehmer ihre jeweiligen Identifier **UUID$_{Ai}$**, **UUID$_{Bi}$** und **UUID$_{Ci}$** und hören die der anderen mit.

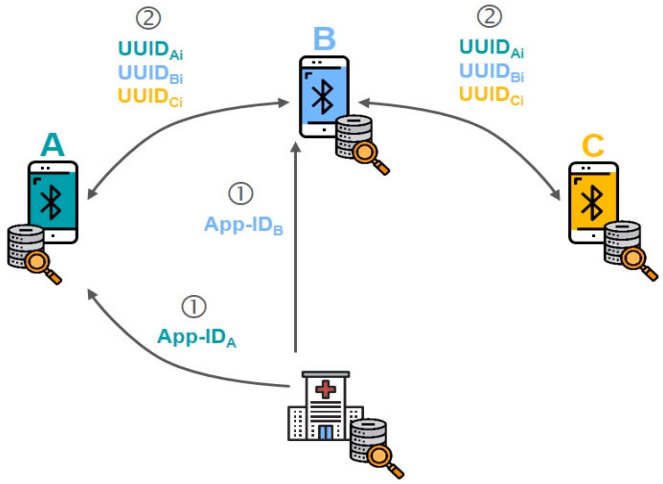

Abbildung 40: Zustand 2 - Austausch von Informationen zwischen den Teilnehmern – UUID

3. Die empfangenen UUIDs werden nicht gespeichert, sondern zusammen mit der eigenen UUID gehasht. Dazu werden die UUIDs der Größe nach sortiert (wichtig, da somit die Reihenfolge bei beiden Teilnehmern gleich ist), konkateniert und gehasht. Im Beispiel sind dies für Teilnehmer **A** die Werte **Hash (UUIDAi, UUIDBi)** und **Hash (UUIDAi, UUIDCi)** als Indikator, dass **A** und **B** bzw. **A** und **C** in Kontakt waren. Die Kontakte werden mit einem Zeitstempel (und ggf. mit weiteren Daten, nicht aber den UUIDs) an die zentrale Stelle geschickt.

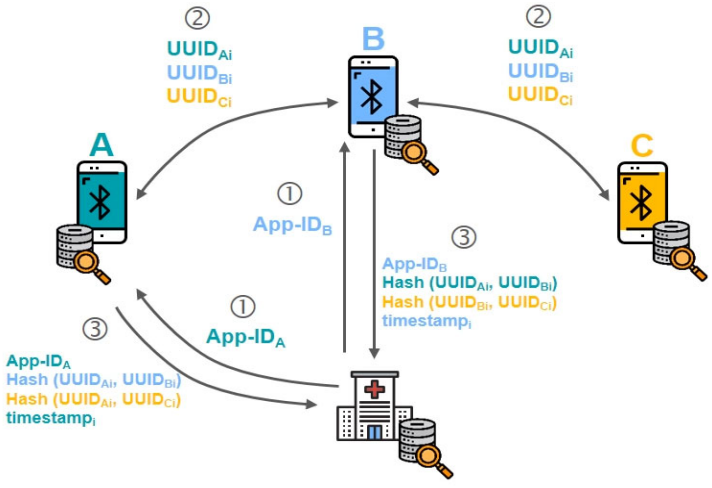

Abbildung 41: Zustand 3 - Hashed der eigenen UUID zusammen mit gesannten UUIDs

4. Im Beispiel wird Teilnehmer **B** positiv auf COVID-19 getestet und die App-ID wird der zentralen Stelle mitgeteilt (verifiziert via App oder Server).

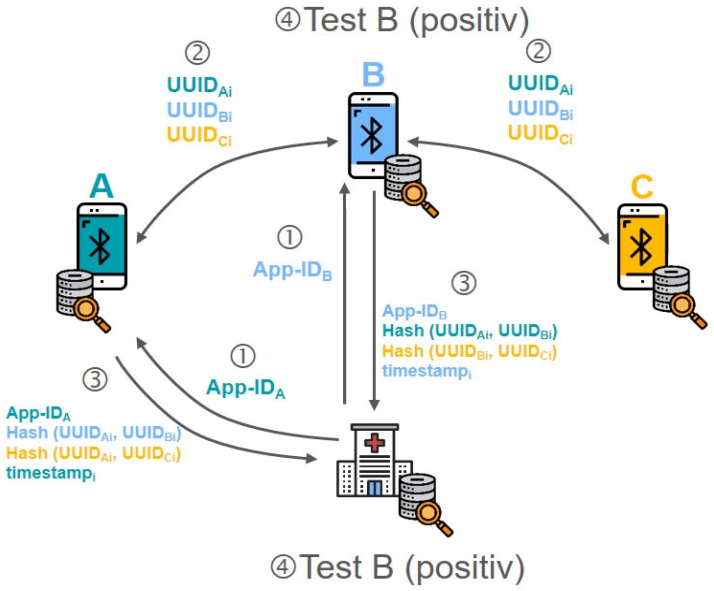

Abbildung 42: Zustand 4 - Teilnehmer B wird positiv getestet

5. Ein Kontakt gilt dann als erfolgt, wenn zwei Teilnehmer identische Hashes senden; der Zeitstempel nicht zum Abgleich, sondern wird nur zur zeitlichen Risikobewertung des Kontaktvorgangs (und letztlich der Aktualität des Datensatzes) benötigt. Darauf aufbauend hat die zentrale Stelle nun die Möglichkeit, Kontakte zu infizierten Personen zu prüfen. Im Beispiel findet die zentrale Stelle für den betrachteten Wert **Hash (UUIDAi, UUIDBi)** tatsächlich die beiden Absender **App-IDA** und **App-IDB**.

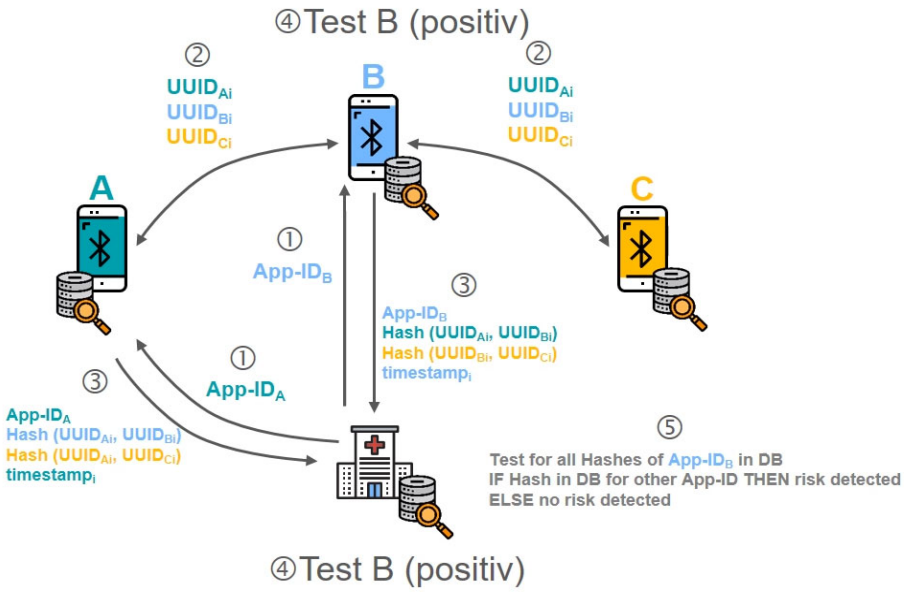

Abbildung 43: Zustand 5 - Prüfung auf Kontakte zum Infizierten

6. Das Ergebnis des Abgleichs sämtlicher solcher Matches wird in die aktuelle Risikobewertung der beteiligten Teilnehmer eingearbeitet (in einem gewissen Grad und ggf. je nach Status des jeweils betrachteten Teilnehmers rekursiv, d.h. die Kontakte von Kontakten erfassend). Der aktuelle Stand der Risikobewertung wird den Teilnehmern (im Beispiel Teilnehmer **A**) verschlüsselt auf Anfrage oder bei Änderung per Push-Message mitgeteilt. Teilnehmer **A** steht es nun frei, unter Vorlage dieser Gesamtbewertung weitere Schritte zu unternehmen.

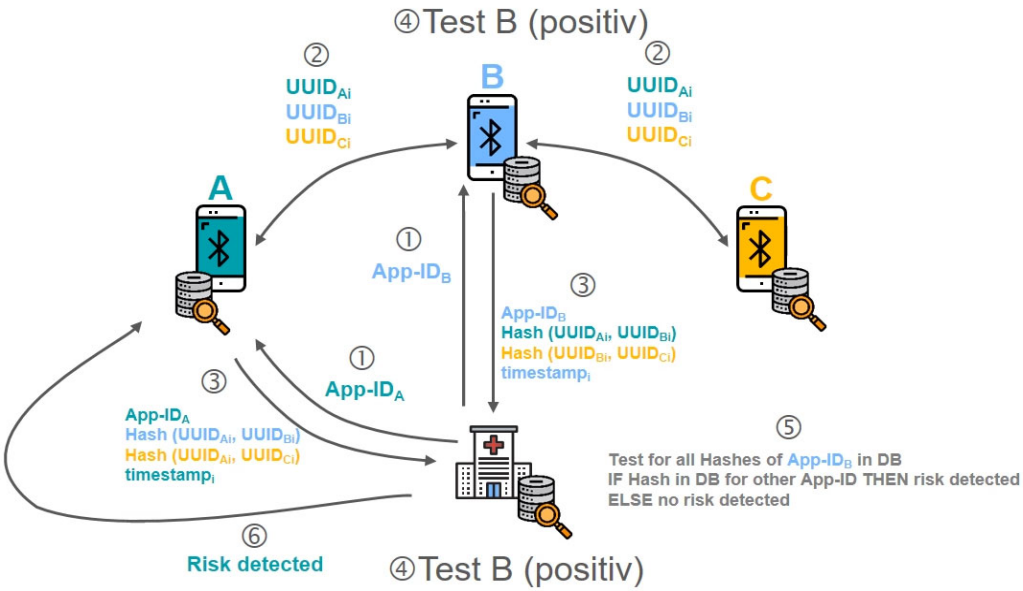

Abbildung 44: Zustand 6 - Rückmeldung des Ergebnisses an Teilnehmer A

5.5.3 Probleme

Es ist auch hier noch zu bewerten, ob ein böswilliger Nutzer nicht trotz anonymer App-ID eine direkte Beziehung zum Smartphone eines gegenüberstehenden Kontaktpartners herstellen kann. Er „sieht“ im Moment des Kontakts unweigerlich auch dessen per Bluetooth ausgesendete UUID und kann den von ihm eigentlich anonymisiert gespeicherter Kontakt später ggf. wieder einem Smartphone 1:1 via UUID zuordnen.

5.5.4 Vorteile

- Auf normalem Wege (Nutzung der offiziellen App) kein Rückschluss auf Gerät, keine Korrelation möglich
- Gezielte Angriffe durch Korrelation mit weiteren Daten zwar grundsätzlich möglich, aber nur mit erheblichem technischem Aufwand und nur für einen Tag.
- Anwender können nicht den Infektionsstand eines anderen abfragen, sondern nur den eigenen Kontakt zu solchen Infizierten.
- Die Authentifizierung erfolgt über die generierte App-ID.

5.5.5 Nachteile

- Die zentrale Stelle hat alle Informationen und ein Bekanntwerden des Zusammenhangs App-ID zu Teilnehmer kann die Anonymität aufheben und die Kontakte (mit wem und wann) eines Teilnehmers u.U. offengelegt werden.

5.5.6 Bewertung

Der Vorteil der Lösung ist, dass hier eine statistische Gesamtauswertung gemacht werden kann, inklusive der Kontaktdauer der Teilnehmer. Der Nachteil ist, dass die zentrale Stelle alle Informationen hat und ein Bekanntwerden des Zusammenhangs App-ID zu Teilnehmer die Anonymität aufhebt und die Kontakte (mit wem und wann) eines Teilnehmers u.U. offengelegt werden.

5.6 Ergänzung zu allen vorgeschlagenen Ideen: SSL-Zertifikate

Bei einigen der vorgestellten Umsetzungsideen gibt es zwei gemeinsame Anforderungen:

- Die Datenübertragung zwischen dem Smartphone und der zentralen Stelle muss verschlüsselt ablaufen.
- Das Smartphone soll sich bei dieser Datenübertragung authentifizieren, so dass sichergestellt ist, welches Gerät Daten an die zentrale Stelle sendet oder von dieser zentralen Stelle abfragt.

Eine mögliche Lösung dafür ist die Nutzung von TLS-Zertifikaten, die – grob skizziert – so ablaufen könnte:

1. Beim Installieren der App erzeugt die App ein RSA Schlüsselpaar
2. Dazu errechnet die App einen Hashwert der eigenen UUID
3. Diese gehashte UUID wird als Common Name (ähnlich einem Server-Namen oder einer IP) in einen Certificate Signing Request (CSR) mit dem Public Key der UUID an die zentrale Stelle (pro Land) übermittelt, die gleichzeitig als Certification Authority (CA) fungiert.
4. Die CA signiert mit ihrem eigenen Private Key und schickt das Zertifikat an das Smartphone zurück.
5. Die zentrale Stelle kennt also nicht die UUID im Klartext, sondern nur die gehashte UUID. Die Zentrale weiß aber, dass dieses Smartphone die App verwendet. Außerdem kennt die zentrale Stelle den Public Key dieses Smartphones.
6. Bei der späteren Übermittlung von Informationen an die zentrale Stelle oder bei der Abfrage von Kontakten bzw. deren Infektionszustand verschlüsselt das Smartphone die übermittelten Daten mit dem eigenen Private Key. Die Zentrale entschlüsselt diese Abfrage mit dem Public Key, der zu der gehashten UUID gehört. Damit ist das Smartphone auch authentifiziert.

5.7 Bewertung der Umsetzungsideen im Vergleich

In diesem Kapitel soll eine Matrix mit Gegenüberstellung der Features und Auswirkungen im Bereich Datenschutz, Privacy, IT-Sicherheit, statistischer Auswertungsmöglichkeit bzw. Berechnung des individuellen Infektionsrisikos die Unterschiede zwischen den verschiedenen Lösungsideen visualisieren und die Entscheidungsfindung für oder gegen eine Lösung erleichtern.

Die Idee 0 – Klarnamen ist im Dokument nicht beschrieben worden, da eine Authentifizierung bzw. Verknüpfung von Gesundheitsdaten mit dem Klarnamen oder einfach auf eine Person zurückzuführende Merkmalen dem Grundgedanken der Initiative diametral gegenübersteht. Für den Vergleich in der Matrix ist sie jedoch hilfreich.

Idee	Key-Features	Datenschutz und Privacy	IT-Sicherheit	Persönliches Infektionsrisiko	Statistische Gesamtbetrachtung[10]	Resistenz gegen Angriffe / Abfragen durch Dritte
0: Klarnamen	Login mit Klarnamen (z.B. Usernamen, E-Mail-Adresse) – im Dokument nicht behandelt	--	-	++	O	++
1: Plain UUID	UUIDs werden im Klartext lokal und auf dem Server gespeichert	-	-	++	O	--
2: Hashed UUID	UUIDs werden gehashed lokal und auf dem Server gespeichert	-	+	++	O	O
3: Random & UUID	Zusätzliche Verschleierung der UUIDs	O	+	++	O	O
4: Hashed Temporary-ID	Täglich wechselnde Identitäten	++	++	++	O	++
5: Independent Application-ID	Häufig wechselnde Identität	+	++	++	++	+

Bewertungsschema: ++ : sehr gut / + : gut / o : durchschnittlich / - : schlecht bzw. verbesserungsfähig / -- : sehr schlecht / mangelhaft bis ungenügend

[10] Bei den Lösungen 1 bis 4 wird die Überprüfung des eigenen Status durch den Teilnehmer angestoßen, was eine statistische Gesamtbetrachtung erschwert. Grundsätzlich sind alle vier Lösungen jedoch recht einfach umzubauen, so dass die Überprüfung bei jedem Kontakt oder in regelmäßigen Abständen automatisiert erfolgt, wodurch die Qualität des Datenschutzes zwar verschlechtert wird, eine statistische Gesamtbetrachtung dafür jedoch ermöglicht wird (siehe dazu auch Ausführung in Kapitel 4.2).

6 Entwicklungsgrundlagen

6.1 Datenschutz und IT-Sicherheit

6.1.1 Lokale Datenspeicherung

Alle Protokollierungen, Berechnungen und eigene Auswertungen müssen auf dem Smartphone des Nutzers erfolgen. Die hierbei gewonnenen Daten müssen nach dem Stand der Technik verschlüsselt abgelegt werden und dürfen nicht auf einfache Weise von Dritten auslesbar oder fälschbar sen. Der Nutzer muss die volle Hoheit über die Daten haben und diese bei Bedarf vollständig und unwiederbringlich löschen können und dürfen.

6.1.2 Automatische Löschung

In Abhängigkeit der Empfehlung von Virologen sollten sinnvolle und datenschutzkonforme Löschfristen festgelegt werden, innerhalb derer die erfassten Daten sowohl in der App als auch in der Server-Komponente automatisiert gelöscht werden.

Hierbei ist zu beachten, dass es aufgrund der zu erwartenden, lang andauernden Phase der „Corona“-Pandemie sinnvoll sein kann, Teile der Daten über einen längeren Zeitraum vorzuhalten, als reine Kontaktdaten. So ist abhängig von der wissenschaftlichen Einschätzung eine ausgeheilte Covid-19-Erkrankung mit einer anschließenden zeitweisen Immunisierung (ähnlicher einer später ggf. möglichen Impfung) ein Indikator für einen unkritischen Kontakt.

6.1.3 Trennung von Verbindungsdaten

Bei der Kommunikation der App mit dem Server wird es nicht auszuschließen sein, dass weitere technische Merkmale in Verbindungslogs zwischengespeichert werden. Diese Verbindungsdaten sind z.B. TCP/IP-Adressen, die durch Internet- bzw. Mobilfunkbetreiber vergeben werden, IMEI-Adressen, MAC-Adressen der Netzwerkkarten usw. Diese Daten müssen streng getrennt von den Bluetooth-UUIDs oder anderen Identifiern gehalten werden und dürfen keinesfalls nachträglich mit geringem Aufwand hinzuaggregiert werden können. Dies würde dann doch zu einer Identifizierung des einzelnen Smartphones und letztlich dessen Nutzers führen.

6.1.4 Kontrolle durch Sachverständigen- bzw- Ethikrat

Die Einhaltung dieser Maßstäbe muss von unabhängiger Seite (Nicht-staatlicher Ethik- bzw.- Expertenrat) jederzeit überprüfbar sein und überprüft werden!

Diese Kontrollinstanz muss u.a. auch prüfen und darauf hinwirken, dass Hersteller von Smartphone ihnen ggf. vorliegende bzw. von ihnen zu ermittelnde Verknüpfungen zwischen Bluetooth UUID, MAC-Adresse oder gar dem Benutzernamen nicht an Dritte weitergeben bzw. zu eigenen Zwecken ausnutzen.

6.2 Transparenz und Backdoor-Freiheit

Das gleiche gilt für die Offenlegung des Quellcodes und der Gewährleistung einer Backdoor-Freiheit. Entscheidend für die Akzeptanz der App und deren Rechtmäßigkeit (zumindest im Umfeld der Bundesrepublik Deutschland bzw. der EU) ist, dass der Code sowohl der App als auch der zentralen Server- und Infrastrukturkomponenten keinerlei Hintertüren oder versteckte Funktionalitäten enthält. Dies muss durch Veröffentlichung des jeweils aktuellen Quellcodes jederzeit von jedermann prüfbar sein. Gleichzeitig muss sichergestellt werden, dass der Code nicht zu einem späteren Zeitpunkt im Rahmen von Updates unzulässig manipuliert wird (weder durch staatliche Organisationen noch durch Hacker).

Sollte das System über Ländergrenzen hinaus ggf. sogar weltweit eingesetzt werden, ist sicherzustellen, dass sich alle Nutzer und alle teilnehmenden Staaten an diese Regeln halten. Ist dies nicht möglich bzw. bestehen erhebliche Zweifel daran, so sind deren Daten bzw. Systeme so zu separieren, dass es keinen Zugriff auf Systeme aus anderen Rechtskreisen geben kann.

6.3 KISS – Keep it stupid and simple

Die Entwicklung sollte sowohl aus Gründen der Nachprüfbarkeit, der Wartbarkeit und im Hinblick auf den knappen Zeitrahmen nach dem Prinzip „KISS - Keep It Stupid and Simple“ erfolgen, um die Wartbarkeit und Prüfbarkeit zu erhöhen. Es ist von einer stark agilen Entwicklungsmethode auszugehen.

6.4 Rechtliches

Rechtliche Fragestellungen sollten mit Rechtsanwälten und Verfassungsrechtlern diskutiert werden.

Grundsätzlich sollte die Nutzung des Systems auf Freiwilligkeit beruhen. Hierbei besteht jedoch die Gefahr bzw. das Problem, dass nicht genügend Menschen das System nutzen. Sollte der Staat sich dazu entscheiden, dem Gesundheitsschutz und der Seuchenprävention den Vorrang vor Freizügigkeit und Datenschutz zu gewähren, ist das Konzept dennoch verwendbar. In diesem Fall wäre die Installation der Software verpflichtend und das Mitführen des Smartphones in der Öffentlichkeit rechtlich vorzuschreiben. Im Gegenzug würden für die Bürger dann die Ausgangsbeschränkungen gelockert.

Unabhängig davon, ob die Nutzung auf freiwilliger oder verpflichtender Basis erfolgt, muss das gesamte System vollkommen transparent aufgebaut und prüfbar sein. Die hier postulierten Anforderungen hinsichtlich Anonymisierung bzw. Pseudonymisierung dürfen nicht aufgeweicht werden.

6.5 Wissenschaftlicher Austausch

Es ist naheliegend und bekannt, dass es bzgl. des Themas Mobilfunküberwachung zur Seuchenprävention bereits Überlegungen und Ideen an anderer Stelle gibt bzw. geben wird. Der Austausch mit ebenfalls hieran arbeitenden Institutionen sollte unbedingt gefördert und durchgeführt werden, um die Qualität der finalen Lösung zu maximieren und Fehlentwicklungen frühzeitig entgegenzutreten.

Hier sind nach derzeitigem Kenntnisstand vor allem folgende Punkte zu nennen:

- Forschungsregion Heinsberg (Epizentrum des ersten „Corona“-Ausbruchs in der Bundesrepublik Deutschland)
- Ergebnisse des Hackathon der Bundesregierung vom 20. bis 22.03.2020
- App-Entwicklung PEPP-PT: Pan-European Privacy-Preserving Proximity Tracing (u.a. Heinrich-Hertz-Instituts und Robert-Koch-Instituts[11], die lt. Süddeutsche vom 31.03.2020 bzw. Tagesschau vom 01.04.2020 offenbar an einem ähnlichen Konzept wie dem hier vorliegenden arbeiten.
- Anforderungskatalog[12] des Chaos Computer Club zur Entwicklung einer „Corona“-App

Insbesondere das Projekt PEPP-PT scheint ähnliche Ziele zu verfolgen, wie die Cybersec-Fokusgruppe des digitalHUB Aachen und daher soll dem Team angeboten werden, deren Lösung mit den Überlegungen auf hiesiger Seite abzugleichen und insbesondere in den Bereichen IT-Sicherhit und Datenschutz zu bewerten.

6.6 Finanzierung

Der Finanzbedarf für die Umsetzung ist derzeit nicht abschätzbar. Aufgrund der Dringlichkeit, ein wirksames Werkzeug zur Eindämmung der Infektionen zu finden, sollten die Kosten jedoch vollkommen irrelevant sein. Hier ist der Staat bzw. die Allgemeinheit gefordert, durch eine schnelle und unbürokratische Zurverfügungstellung von ausreichenden Geldmitteln die Entwicklung und den Betrieb sicherzustellen. Gelingt es, mit der App einerseits die Bewegungsfreiheit der Menschen wieder zu erhöhen und das öffentliche Leben weitestgehend normalisieren zu können, ist der wirtschaftliche Nutzen um ein Vielfaches höher als der Aufwand – vom Retten von Menschenleben mal ganz abgesehen.

Mögliche Finanzierungsmethoden:

- Staatliche Förderung durch Land / Bund / Ministerien
- Förderung durch EU-Mittel
- Kickstarter- oder Sciencestarter Finanzierung durch Community (Schwarm)
- Sponsoring durch Unternehmen
- Spenden von Nutzern
- Sach- und Personalleistung durch Firmen und Personen, die unentgeltlich mitwirken.

Wünschenswert ist, dass das Projekt für die aktiv beteiligten Personen und Institutionen auskömmlich ist, damit die Motivation in Krisenzeiten jetzt zu 100% in das Projekt einzusteigen entsprechend hoch ist. Eine spätere Finanzierung durch Crowdfunding ohne stattliche Hilfe ist in der aktuellen Ausnahmesituation nicht vollkommen undenkbar und würde – entsprechende PR-Unterstützung durch Medien und öffentlichkeitswirksame Darstellung vorausgesetzt – ggf. auch zum Erfolg führen, wenn eine kritische Masse von Nutzern erreicht würde.

[11] https://www.sueddeutsche.de/digital/“Corona“virus-smartphone-app-bluetooth-datenschutz-1.4862314 und https://www.tagesschau.de/inland/“Corona“virus-handydaten-101.html
[12] https://www.ccc.de/en/updates/2020/contact-tracing-requirements

6.7 Zeitplan

Das zur Verfügung stehende Zeitfenster ist extrem knapp. Damit die App einen entscheidenden Beitrag für mehr Transparenz bzw. der Infektionszahlen und der Verbreitung des Virus liefern kann, muss eine funktionsfähige Version kurzfristig in Betrieb gehen können. Nur so kann hierdurch ein Beitrag für eine Lockerung der Ausgangs- und Kontaktsperren geleistet und dazu beigetragen werden, dass sich das öffentliche Leben schrittweise wieder normalisieren kann. Es gilt hierbei, durch den Einsatz der App den Ausbruch weiterer – ggf. stärkerer – Infektions- incl. saisonaler Grippewellen zu verhindern und ein Werkzeug zu liefern, um mit dem Virus in den kommenden Jahren zu leben, bis es einen Impfstoff und/oder eine wirksame Therapie gibt. Trotz aller gebotenen Eile gilt der Grundsatz „Sorgfalt vor Schnelligkeit“, denn andere gut gemeinte Beispiele aus dem Bereich der „Corona“-Hilfen haben gezeigt, dass schnell aufgesetzte Systeme ebenso schnell von Angreifern für ihre Zwecke missbraucht werden (Bespiel Website für die Beantragung der „Corona“-Hilfe ohne jegliche Legitimierungsprüfung wurde von Hackern imitiert).

6.8 Team

Für die Realisierung einer konkreten Lösung werden u.a. folgende Personen, Funktionen, Skills und Institutionen benötigt:

- Projektleiter
- App-Programmierer
- Infrastrukturanbieter (Server, Netzwerk)
- Oberflächenentwickler
- Datenbankprogrammierer
- Security-Architekten
- Pen-Tester
- Rechtsanwälte / Verfassungsrichter
- Datenschutzfachleute
- Presse
- Netzaktivisten (CCC)
- PR-Agentur
- Politiker
- Geldgeber
- Virologen
- Ethikrat
- Sachverständige für Audits
- Gesundheitsbehörden
- Innenministerium /Gesundheitsministerium
- Wissenschaftler (FH/RWTH)

6.9 Eigentums-, Nutzungs- und Verwertungsrechte

Die App soll überregional / weltweit zur Nutzung freigegeben werden. Die Rechte daran sollen Public Domain sein.

6.10 Ausblick

Die App sollte wenn möglich technologie-offen entwickelt werden, damit sie ggf. auch ohne Bluetooth funktioniert.

Bei der Zielsetzung sollte man sich nicht allein nur auf das aktuelle „SARS-CoV-2-Virus beschränken, sondern auf alle ähnlichen, denkbaren Epidemien. Daher wäre es im Datenmodell sinnvoll, bei jedem Test / positiven Kontakt zu hinterlegen, um welches Virus (Version) es sich handelt.

7 About

7.1 Über die Fokusgruppe Cyber-Security im digitalHUB Aachen

Die Fokus-Gruppe will in den Themenbereich Cybersicherheit Transparenz bringen und in Unternehmen eine entsprechende Awareness schaffen. Dabei sollen auch entsprechende Veranstaltungsformate für die Aachen Area realisiert werden. Gleichzeitig bietet die Gruppe eine Plattform zum informellen Austausch.

Die Fokusgruppe Cyber-Security bündelt als Initiative im digitalHUB Aachen e.V. die Erfahrung und Kompetenz verschiedener Unternehmen und Hochschuleinrichtungen aus dem Bereich Cyber-Security mit dem Ziel, Unternehmen in allen Fragen des Datenschutzes und der Informationssicherheit zu beraten. Die Fokusgruppe nimmt an relevanten Veranstaltungen der Cyber-Security teil und unterstützt die Organisation des nächsten IHK Sicherheitstages NRW am 02. Dezember 2020 in Aachen.

In einem eigenen Workshop-Format bietet die Fokusgruppe die Möglichkeit, technische und finanzielle Aspekte der Cyber-Security von Unternehmen und Organisationen gemeinsam mit Geschäftsführern und Fachverantwortlichen zu diskutieren.

Initiator/Sprecher: Dr. Walter Plesnik, Ingenieurbüro Dr. Plesnik GmbH
Vertreter: Hartmut Blumberg, Institut für IT-Sicherheit GmbH

Kontakt:
Postanschrift:
digitalCHURCH
Jülicher Strasse 72a
D-52070 Aachen

E-Mail: fokusgruppe@plesnik.de

Website: https://aachen.digital/digitalhub-aachen/fokusgruppen/fokusgruppe-cyber-security/

Telefon (Dr. Walter Plesnik)
Tel. +49 241 149 46 0

7.2 Über die Autoren

An der Erstellung des Dokumentes haben folgende Autoren mitgewirkt:

Dipl.-Ing. Thomas Käfer, M.Sc - Würselen

Käfer IT Systeme e.K.
Öffentlich bestellter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung
Master of Science Digitale Forensik
Betrieblicher Datenschutzbeauftragter

Prof. Dr. rer. nat. Marko Schuba - Aachen

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik
FH Aachen - University of Applied Sciences
Institut für Digitalisierung Aachen (IDA)

Dipl.-Ing. Norbert Hamel - Aachen

Bridge:com
Splunk Professional Services Consultant and Instructor
Splunk Certified Administrator and Architect
Splunk Certified Enterprise Security Consultant

Dipl.-Ing. Markus Jansen - Würselen

QM Security Engineer – LANCOM Systems GmbH

Dr. Walter Plesnik - Aachen

Geschäftsführer Ingenieurbüro Dr. Plesnik GmbH
Business Transformation Manager
Sprecher der Fokusgruppe Cyber-Security im Digital Hub, Aachen

8 Index

8.1 Stichwortverzeichnis

8.2 Abbildungsverzeichnis

8.3 Quellenverzeichnis und weiterführende Links

Quellen siehe Fußnoten bzw. Bildunterschriften

Titelbild: Fotolia – lizenziert über KäferLive – Thomas Käfer

8.4 Piktogramme

Piktogramme sollen einheitlich verwendet werden.

Achtung: Kennzeichnet wichtigen Hinweis

Obsolet/Gelöscht: Kennzeichnet gelöschte bzw. zukünftig nicht mehr gültige Passage (ggf. zusammen mit durchgestrichenem Text); Kennzeichnung und gestrichene Passage in nächster Version entfernen

Zur Diskussion / noch nicht abschließend geklärter/entschiedener Punkt

Neu: Neu hinzugefügte Passage (Kennzeichnung in nächster Version entfernen)

Die Piktogramme werden jeweils mit umlaufendem Text gesetzt (siehe oben):

8.5 Änderungshistorie

Datum	Version	Autor	Änderung
14.04.2020	V 1.0.1	Thomas Käfer	Watcher und Player in 4.2 vertauscht
14.04.2020	V 1.0	Alle	QS, Freigabe Dokument zur Veröffentlichung; Kapitel 4. 2 ergänzt
13.04.2020	V 0.11	Markus Jansen, Marko Schuba, Norbert Hamel, Thomas Käfer	Lösungsidee 5 ausformuliert: QS, Kapitel mit Übersichtsmatrix und Bewertungen ergänzt; Idee Crossed Hashed UUID verworfen
09.04.2020	V 0.10	Alle	Verabschiedung Abstract; Vorabveröffentlichung digital-HUB
09.04.2020	V 0.9	Marko Schuba, Markus Jansen, Norbert Hamel	Ergänzung Lösungsideen Kapitel 5
08.04.2020	V 0.8	Thomas Käfer	Diskutierte und optimierte Lösungsideen visualisiert
07.04.2020	V 0.7	Marko Schuba	Neue Lösungsidee
06.04.2020	V 0.6	Norbert Hamel, Thomas Käfer	Ergänzungen
06.04.2020	V 0.5	Thomas Käfer, Markus Jansen, Walter Plesnik	Fehlerkorrekturen und Ergänzungen
03.04.2020	V 0.4	Thomas Käfer mit Input Prof. Marko Schuba, Norbert Hamel, Dr. Walter Plesnik und Markus Jansen	Kapitel 4.4 hinzugefügt; Abstract geändert; Index hinzugefügt; Kap. 5.5 Wissenschaftlicher Austausch ergänzt; CV hinzugefügt, Layout überarbeitet
02.04.2020	V 0.3	Thomas Käfer	Überarbeitung und Ergänzung in Details
01.04.2020	V 0.2	Thomas Käfer	Überarbeitung / QS
31.03.2020	V 0.1	Thomas Käfer	Formulierung Projektidee und Anlage Grunddokument