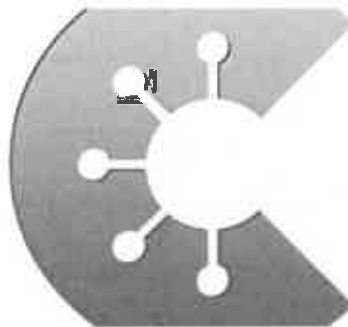


**SAP DEUTSCHLAND SE & CO. KG
T-SYSTEMS INTERNATIONAL GMBH
UND
BUNDESREPUBLIK DEUTSCHLAND
VERTRETEN DURCH DAS
BUNDESMINISTERIUM FÜR GESUNDHEIT**

**PROJEKT CORONA WARN APP
ABSTIMMUNGSVEREINBARUNG**



Inhalts- und Anlagenverzeichnis

Präambel	4
1. Vertragsgegenstand	5
1.1 Entwicklung der Corona Warn App	5
1.2 Informationsaustausch und Abstimmung über Schnittstellen	5
1.3 Kein Konsortium	5
2. Abgrenzung der Leistungen der Parteien	6
2.1 Übersicht zur Leistungsabgrenzung	6
2.2 Aufgaben und Leistungsumfang der SAP	6
2.3 Aufgaben und Leistungsumfang der T-Systems	6
2.4 Festlegung der Schnittstellenspezifikationen	7
2.5 Support- / Pflege-Weiterentwicklung	7
3. Anforderungen des Auftraggebers	8
3.1 Allgemeine Anforderungen	8
3.2 Verhältnis zu Projektverträgen	9
4. Zusammenarbeit der Parteien	9
4.1 Projektorganisation und -durchführung	9
4.2 Informationsaustausch und Informationspflicht	9
4.3 Beziehung Dritter	9
4.4 Grundsätze bei direkter Abstimmung zwischen SAP und T-Systems	9
5. Entwicklungsphase	10
5.1 Abstimmung mit BSI und BfDI	10
5.2 Dokumentation und Zertifikate	10
6. Inbetriebnahme und Abnahme	11
6.1 Vorbereitung der Betriebsbereitschaft	11
6.2 Integrations- und Funktionsprüfung	11
6.3 Freigabe zur Aufnahme des Wirkbetriebs	12
7. Change Request-Verfahren	14
7.1 Änderungsverlangen des Auftraggebers	14
7.2 Änderungsvorschlag von SAP und/oder T-Systems	15
7.3 Allgemeine Bestimmungen	15
8. Haftung	15
8.1 Haftung der Industriepartner gegenüber dem Auftraggeber und Dritten	15
8.2 Haftung der Industriepartner untereinander ohne Drittbezug	16
8.3 Erstreckung der Haftungsbegrenzung im Verhältnis zum Auftraggeber	16
9. Nutzungsrechte	16
9.1 Keine direkte Einräumung von Nutzungsrechten	16
9.2 Nutzungsrechte unter Projektverträgen	16
10. Geheimhaltung	16
10.1 Nutzung vertraulicher Informationen	16
10.2 Geheimhaltungsmaßnahmen	17
10.3 Ausnahmen	17
10.4 Entfall	17

10.5	Dauer der Geheimhaltungsverpflichtung	17
11.	Datenschutz	18
12.	Allgemeine Bestimmungen	18
12.1	Keine gesonderte Vergütung / Kostentragung	18
12.2	Laufzeit / Beendigung	18
12.3	Schlussbestimmungen	18
Anlage 1	Spezifikationen	21
Anlage 2	Fehlerbehebungsprozesse für CWA-Backend- und Frontend-Teil	22
Anlage 3	Governance	23
Anlage 4	Dokumentation	24
Anlage 5	Abnahmekriterien und -Prüfungen	25
Anlage 6	Änderungsverfahren	26

Diese

ABSTIMMUNGSVEREINBARUNG

wird zwischen

- (1) der Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit, Friedrichstraße 108, 10117 Berlin ("Auftraggeber"),
- (2) SAP Deutschland SE & Co. KG, Hasso-Plattner-Ring 7, 69190 Walldorf ("SAP") und
- (3) T-Systems International GmbH, Hahnstraße 43, 60528 Frankfurt am Main ("T-Systems" oder "TSI")

geschlossen. Der Auftraggeber, SAP und T-Systems werden nachstehend gemeinsam als die "Parteien" und jeweils einzeln auch als "Partei" bezeichnet. SAP und T-Systems werden gemeinsam und jeweils einzeln auch als "Industriepartner" bezeichnet.

PRÄAMBEL

- (A) Die Unterbrechung von Infektionsketten ist der wesentliche Mechanismus zur Bekämpfung der weiteren Ausbreitung des Corona-Virus. Digitale Anwendungen können hierbei einen erheblichen Beitrag bei der Identifikation und Information möglicher Kontaktpersonen leisten.
- (B) Ein vielversprechender Ansatz hierbei ist die Identifikation und Dokumentation relevanter Kontakte mittels Smartphone / Bluetooth LE. T-Systems und SAP haben sich als Industriepartner bereiterklärt, die bisherigen Forschungsergebnisse in ein die fachlichen Anforderungen sowie die Vorgaben an Datenschutz und Informationssicherheit erfüllendes Endprodukt zur überführen und dessen infrastrukturellen Betrieb über die Entwicklungsphase hinaus zu gewährleisten ("Projekt Corona Warn App"). Hierbei besteht ausdrücklich die Offenheit der beiden Industriepartner, das Produkt mit weiteren gebotenen Nachentwicklungen auf Basis fachlicher Anforderungen voran zu treiben.
- (C) Vor diesem Hintergrund hat der Auftraggeber mit SAP einen Vertrag über Entwicklungs- und Pflegeleistungen im Projekt Corona Warn App ("SAP-Vertrag") und mit der T-Systems einen Vertrag über IT-Leistungen im Projekt Corona Warn App ("T-Systems-Vertrag") geschlossen. Das unter diesen Verträgen von SAP und T-Systems entwickelte und zum Betrieb bereitgestellte System zum Betrieb der Corona Warn App wird nachstehend insgesamt als "Gesamtsystem" bezeichnet. Der SAP-Vertrag, der T-Systems-Vertrag und diese Abstimmungsvereinbarung werden zusammen als die "Projektverträge" und jeweils einzeln auch als "Projektvertrag" bezeichnet.
- (D) Die Parteien sind sich bewusst, dass die Entwicklung und der Betrieb der Corona Warn App sowohl hinsichtlich der spezifischen Anforderungen, der Einbindung Dritter als auch aufgrund der zeitlichen Kritikalität besondere Herausforderungen nicht nur an die Parteien, sondern an alle an diesem Projekt unmittelbar oder mittelbar Beteiligten stellt

und ohne ein zügiges und konstruktives Zusammenwirken aller Beteiligten nicht abgeschlossen werden kann.

- (E) Vor diesem Hintergrund möchten die Parteien in dieser Abstimmungsvereinbarung gemeinsame Regelungen und Prozesse sowie einen Rahmen für ihre Zusammenarbeit im Projekt Corona Warn App vereinbaren.

1. VERTRAGSGEGENSTAND

1.1 Entwicklung der Corona Warn App

Die Industriepartner wollen auf Basis jeweils gesonderter Verträge mit dem Auftraggeber eine Tracing-App entwickeln und betreiben, um Kontaktpersonen von Corona-Infizierten warnen zu können. SAP und T-Systems erbringen hierzu gesonderte Leistungen gegenüber dem Auftraggeber. Es ist nicht vorgesehen, eine Gesamtleistung zu erbringen oder eine Gesamtverantwortung durch die Industriepartner gegenüber dem Auftraggeber zu übernehmen. Ebenso soll eine Haftung für die Leistung des jeweils anderen Industriepartners ausgeschlossen werden. Jeder Industriepartner haftet vielmehr für seinen jeweiligen Leistungsbeitrag alleine.

1.2 Informationsaustausch und Abstimmung über Schnittstellen

Für die Erbringung der jeweiligen Leistungsanteile und für die Funktionsfähigkeit der Anti-Corona-App ist ein gegenseitiger Informationsaustausch und die Abstimmung über Schnittstellen zwischen den Parteien erforderlich. Der Informationsaustausch und die Abstimmung über Schnittstellen oder sonstige Leistungsinhalte und etwaige Zulieferungen erfolgen nach den Bestimmungen dieser Abstimmungsvereinbarung.

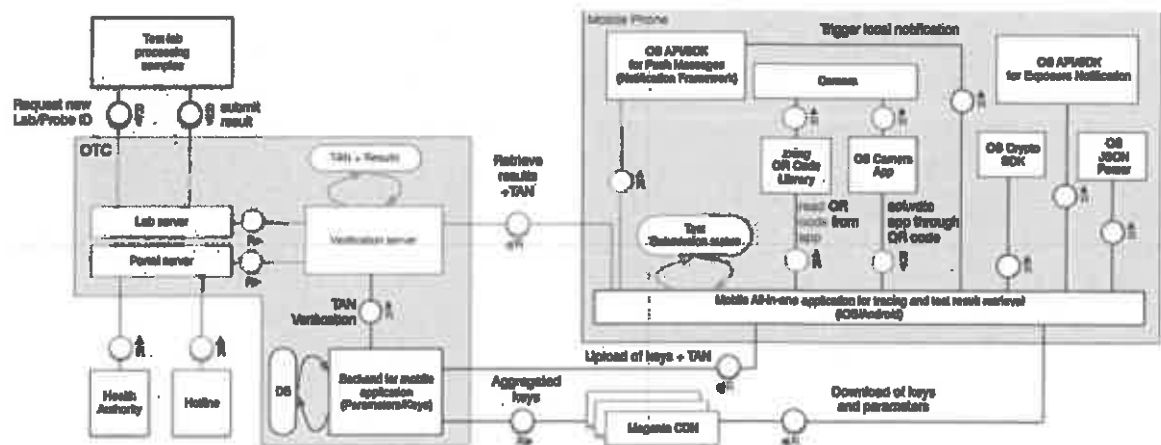
1.3 Kein Konsortium

Mit dieser Abstimmungsvereinbarung wird weder eine konsortiale Beziehung zwischen den Industriepartnern begründet, noch ist eine gesellschaftsrechtliche Verbindung beabsichtigt.

2. ABGRENZUNG DER LEISTUNGEN DER PARTEIEN

2.1 Übersicht zur Leistungsabgrenzung

In der nachfolgenden Darstellung sind die Leistungsbereiche der Industriepartner schematisch dargestellt:



Stand: 2020-05-08 16:00

Die Leistungsbereiche von SAP sind blau markiert, die Leistungsbereiche von T-Systems sind magenta markiert.

2.2 Aufgaben und Leistungsumfang der SAP

Die Leistungen der SAP ergeben sich aus dem SAP-Vertrag. Diese umfassen insbesondere:

2.2.1 Design und Entwicklung der Corona-Warn-App (iOS und Android); basierend auf einem neuen SDK, das von Apple und Google zur Verfügung gestellt wird und als Exposure Notification Framework bezeichnet wird

2.2.2 Entwicklung des Backends zur Entgegennahme von Upload-Anfragen der Clients (Tracing Server); Übergabe von Konfigurationsparametern an die mobilen Anwendungen und Zusammenfassung der Diagnoseschlüssel in Blöcke

2.2.3 Publizieren der wesentlichen Projektbestandteile als Open Source auf GitHub

Die verbindlichen Leistungsinhalte vereinbart SAP ausschließlich direkt mit dem Auftraggeber unter dem SAP-Vertrag.

2.3 Aufgaben und Leistungsumfang der T-Systems

Die Leistungen der T-Systems ergeben sich aus T-Systems-Vertrag. Diese umfassen insbesondere:

- 2.3.1 Die Entwicklung und den Betrieb des Verifikationsservers, des Lab Servers sowie des Portal Servers innerhalb des Prozesses zur Verifizierung / Falsifizierung einer gemeldeten Infektion,
- 2.3.2 Betrieb des Backends zur Entgegennahme von Upload-Anfragen der Client (Tracing Server),
- 2.3.3 Bereitstellung einer Managed „Platform as a Service“ (PaaS),
- 2.3.4 Hotline Service.

Die verbindlichen Leistungsinhalte vereinbart T-Systems ausschließlich direkt mit dem Auftraggeber unter dem T-Systems-Vertrag.

2.4 Festlegung der Schnittstellenspezifikationen

Die verbindliche Festlegung der Schnittstellenspezifikationen ergibt sich aus Anlage 1. Weitere Festlegungen in Bezug auf die technische Ausgestaltung der Schnittstellen erfolgt in dem hierfür vorgesehenen Abstimmungsgremium gemäß Ziffer 4.1 (Governance).

2.5 Support- / Pflege-Weiterentwicklung

- 2.5.1 SAP erbringt ausschließlich die im SAP-Vertrag beschriebenen Leistungen in Bezug auf Support, Pflege und Weiterentwicklung der Corona Warn App (Features gemäß SAP-Vertrag definiert).
- 2.5.2 Das technische Support Modell für die Corona Warn App ist in drei Level unterteilt. Level 1 und 2 werden von T-Systems bereitgestellt. Level 3 wird von SAP bereitgestellt. Das folgende Bild zeigt eine Beschreibung für jedes Level:

Level 1 (T-Systems)	Level 2 (T-Systems)	Level 3 (SAP)
<ul style="list-style-type: none"> ▪ Proaktive Anwendungsüberwachung und -Alerting ▪ Incident Handling ▪ Dispatching von Problemen ▪ Ticketerstellung 	<ul style="list-style-type: none"> ▪ Ursachenanalyse ▪ Durchführung von Heilungsmaßnahmen ▪ Verwalten und Betrieb der Infrastruktur 	<ul style="list-style-type: none"> ▪ Fehlerbehebung ▪ Optimierung des Codes ▪ Stabilisierungsmaßnahmen ▪ Migrationen ▪ Codeänderungen / Refactoring ▪ Funktionsverbesserungen

Hiervon unabhängig wird von T-Systems eine technische Hotline für die Endnutzer gemäß den Festlegungen im Projektvertrag eingerichtet.

- 2.5.3 Die detaillierten Fehlerbehebungsprozesse für den CWA-Backend-Teil und den Frontend-Teil sind in Anlage 2 detailliert beschrieben.

3. ANFORDERUNGEN DES AUFTRAGGEBERS

3.1 Allgemeine Anforderungen

Ziel des Auftraggebers und Zweck der Projektverträge ist die Erstellung, die Inbetriebnahme und der Betrieb des Gesamtsystems als funktionierende Lösung zur Bekämpfung der Covid-19-Pandemie, welches aus verschiedenen Einzelkomponenten besteht. Vor diesem Hintergrund muss das Gesamtsystem mindestens folgenden Anforderungen genügen ("Allgemeine Anforderungen"):

- 3.1.1 Das Gesamtsystem soll mittels Bluetooth LE Technologie in der Lage sein, andere in Reichweite befindliche Nutzerinnen und Nutzer der Anwendung zu registrieren, den Abstand zueinander zu bestimmen, die Kontakte zu dokumentieren und darauf aufbauend einen vom Robert-Koch-Institut definierten Risikowert einer Infektion zu bestimmen (wobei definierte Parameter im Betrieb angepasst werden können). Hierzu sind funktional lauffähige Applikationen für iOS und Android unter Nutzung der Betriebssystem-internen Schnittstellen bereitzustellen.
- 3.1.2 Die Anwendung soll in der Lage sein, das Ergebnis von SARS-CoV-2-Nachweisen (positiv und negativ) zu verarbeiten und darauf aufbauend mittels der Anwendung registrierte Kontaktpersonen über ihr Infektionsrisiko zu informieren.
- 3.1.3 Das Ergebnis des SARS-CoV-2-Nachweis und das damit einhergehende Auslösen der Warnung an Kontaktpersonen soll über verschiedene Wege realisiert werden können und pseudonym nutzbar sein.
- 3.1.4 Über eine Verifikationshotline soll Nutzerinnen und Nutzer ermöglicht werden, selbstständig einen positiven SARS-CoV-2-Nachweis an die App zu melden.
- 3.1.5 Die Anwendung soll zudem in der Lage sein, das Ergebnis von SARS-CoV-2-Nachweisen (positiv und negativ) durch eine technische Anbindung an die entsprechenden Prüflabore direkt zu verarbeiten. Hierfür wird ein Code genutzt, der innerhalb der Anwendung eine pseudonyme Verknüpfung des Labor-Testergebnisses und der Anwendung ermöglicht.
- 3.1.6 Das Gesamtsystem beinhaltet ein leistungsfähiges Backend, welches die vereinbarte Verfügbarkeit und Skalierbarkeit auf die gesamte Bundesrepublik Deutschland gewährleistet.
- 3.1.7 Sämtliche Komponenten des Gesamtsystems müssen die abgestimmten Anforderungen an Informationssicherheit und Datenschutz erfüllen. Hierzu sind das Bundesamt für Sicherheit in der Informationstechnik und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit durchgehend in den Entwicklungsprozess einzubeziehen.
- 3.1.8 Die App und die Hotline muss den Anforderungen an die Barrierefreiheit in dem im jeweiligen Projektvertrag vereinbarten Umfang genügen.

3.1.9 Neben einer Hotline zur Verifikation des Testergebnisses für die Anwendung ist eine Hotline zu allgemeinen, insbesondere technischen Anfragen bereitzustellen.

3.1.10 Der Betrieb des beschriebenen Gesamtsystems, inkl. notwendiger technischer Weiterentwicklungen zur Gewährleistung der Lauffähigkeit auf mobilen Endgeräten, ist über die Laufzeit der Projektverträge zu gewährleisten.

3.2 Verhältnis zu Projektverträgen

Die Allgemeinen Anforderungen sind von den Industriepartnern in ihrem jeweiligen Leistungsbereich umzusetzen. Abweichende Spezifikation oder Bestimmungen in den jeweiligen Projektverträgen einschließlich deren Leistungsbeschreibungen oder im Rahmen von Change Requests haben Vorrang vor den Allgemeinen Anforderungen.

4. ZUSAMMENARBEIT DER PARTEIEN

4.1 Projektorganisation und -durchführung

Die Parteien haben sich auf die in Anlage 3 niedergelegten Bestimmungen zur Projektorganisation und -durchführung (Governance) verständigt.

4.2 Informationsaustausch und Informationspflicht

4.2.1 Die Parteien werden vertrauensvoll und kooperativ zusammenarbeiten. Jeder Industriepartner wird den anderen Industriepartner unverzüglich über alle Ereignisse hinsichtlich seines Leistungsanteils unterrichten, soweit diese die Erfüllung der dem anderen Industriepartner obliegenden Verpflichtungen berühren oder berühren können.

4.2.2 Die Parteien arbeiten auch bei Anfragen nach dem Informationsfreiheitsgesetz vertrauensvoll zusammen und unterstützen sich jeweils in angemessenem Umfang. Soweit für die Offenlegung von Informationen die Zustimmung der Industriepartner erforderlich ist, ist diese hiermit noch nicht erteilt, sondern muss im Einzelfall eingeholt werden.

4.3 Beziehung Dritter

Der Auftraggeber kann zu sämtlichen Besprechungen, Abstimmungen und Sitzungen Dritte hinzuziehen und mit diesen Informationen und Unterlagen zum Projekt Corona Warn App teilen. Dies umfasst insbesondere auch Vertreter anderer öffentlicher Stellen des Bundes und der Länder wie Vertreter des Bundesamts für Informationssicherheit ("BSI") oder des Bundesbeauftragten für Datenschutz und Informationsfreiheit ("BfDI") sowie Vertreter des Robert Koch-Instituts ("RKI").

4.4 Grundsätze bei direkter Abstimmung zwischen SAP und T-Systems

4.4.1 SAP und T-Systems sind grundsätzlich gehalten, sich im Projekt Corona Warn App gegenseitig zu unterstützen und als Technologiepartner des Auftraggebers auch direkt auszutauschen und abzustimmen. SAP und T-Systems werden hierbei vertrauensvoll und offen zusammenarbeiten.

- 4.4.2 Sofern sich im Rahmen einer Abstimmung zwischen SAP und T-Systems Änderungen des SAP-Vertrags und/oder des T-Systems-Vertrags ergeben (einschließlich technischer Änderungen), sind diese mit dem Auftraggeber über das Change Request-Verfahren abzustimmen und zu vereinbaren.
- 4.4.3 Sofern sich im Rahmen der Zusammenarbeit von SAP und T-Systems im Projekt Corona Warn App Meinungsverschiedenheiten ergeben, werden SAP und T-Systems den Auftraggeber unverzüglich informieren und gemeinsam mit dem Auftraggeber alle zumutbaren Anstrengung unternehmen, um die Meinungsverschiedenheit einvernehmlich zu regeln.

5. ENTWICKLUNGSPHASE

Für die Phase des Projekts Corona Warn App bis zur Inbetriebnahme des Gesamtsystems und Abnahme der Features gemäß SAP-Vertrag ("Entwicklungsphase") vereinbaren die Parteien Folgendes:

5.1 Abstimmung mit BSI und BfDI

Datenschutz- und Sicherheitsaspekte sind für das Gesamtsystem wesentlich. Das Datenschutz- und Sicherheitskonzept wird von SAP und T-Systems im Zuge der Entwicklung des Gesamtsystems und nach Maßgabe der Projektverträge erarbeitet. Für den Erfolg des Projekts Corona Warn App ist eine enge und rechtzeitige Einbindung von und Abstimmung mit dem BSI und dem BfDI erforderlich. SAP und T-Systems werden die jeweiligen Konzepte, einschließlich der verfügbaren technischen Dokumentation, dem BSI und dem BfDI unter Einbindung des Auftraggebers jeweils so früh als möglich zur Durchsicht und Stellungnahme zuleiten. Stellungnahmen von BSI und BfDI sind bei der Entwicklung und Herstellung der Betriebsbereitschaft sowie im späteren Betrieb des Gesamtsystems von SAP und T-Systems in ihrem jeweiligen Leistungsbereich zu beachten und umzusetzen. Sofern sich hieraus wesentliche Abweichungen nach Unterzeichnung der Projektverträge ergeben, sind SAP und T-Systems jeweils vor Ausführung verpflichtet, einen Change Request zu stellen. Das weitere Vorgehen wird dann zwischen den Parteien im Rahmen des Change Request-Verfahrens vereinbart.

5.2 Dokumentation und Zertifikate

- 5.2.1 SAP und T-Systems erstellen im Rahmen der Entwicklung die in **Anlage 4** spezifizierte Dokumentation ("Dokumentation").
- 5.2.2 Bei der Erstellung der Dokumentation muss jeder Industriepartner für seinen Leistungsbereich mitwirken und ist inhaltlich nur für seinen Leistungsbereich verantwortlich. Die Industriepartner stimmen sich hinsichtlich Format und Aufbau der Dokumentation ab, so dass der Auftragnehmer eine konsistente und einheitlich formatierte Dokumentation erhält. Der jeweils für die Konsolidierung einer Dokumentation verantwortliche Industriepartner ist in **Anlage 4** spezifiziert.
- 5.2.3 Die Dokumentation ist in deutscher Sprache zu erstellen, wobei Teile auch in englischer Sprache erstellt werden können, wie in **Anlage 4** festgelegt.

- 5.2.4 Die Dokumentation ist spätestens zu den in Anlage 4 genannten Terminen vorzulegen.
- 5.2.5 Weitergehende Pflichten der Industriepartner aus den jeweiligen Projektverträgen bleiben unberührt.

6. INBETRIEBNAHME UND ABNAHME

6.1 Vorbereitung der Betriebsbereitschaft

- 6.1.1 SAP stellt die Features und die für die Herstellung der Betriebsbereitschaft und den Betrieb in der OTC erforderliche Dokumentation gemäß SAP-Vertrag und in Abstimmung mit T-Systems der T-Systems zur Verfügung. Die T-Systems integriert die Features zur Herstellung der Betriebsbereitschaft in das Gesamtsystem.
- 6.1.2 Im Rahmen der Entwicklung, Integration und Herstellung der Betriebsbereitschaft führen SAP und T-Systems die in Anlage 5 definierten Prüfungen und Tests des Gesamtsystems und seiner Komponenten (zusammen, die "Tests") durch, protokollieren das Ergebnis und erstellen bzw. besorgen die jeweiligen Nachweise / Ergebnistypen (zusammen, die "Testergebnisse") und übermitteln diese an den Auftraggeber.
- 6.1.3 Sofern die vorstehenden Tests nicht bestanden oder in den vorstehenden Tests nicht nur leichte Mängel oder nicht nur unerhebliche Sicherheitsrisiken des Gesamtsystems identifiziert werden, sind diese von SAP und T-Systems in ihrem jeweiligen Leistungsbereich zu beheben und die relevanten Tests – soweit erforderlich – zu wiederholen. Die Pflicht zur Behebung leichter Mängel oder unerheblicher Sicherheitsrisiken bleibt unberührt.
- 6.1.4 Der Auftraggeber ist über die vorstehenden Tests mit angemessenem Vorlauf zu informieren und ist berechtigt, an den Tests teilzunehmen. Etwaige Mitwirkungspflichten des Auftraggebers im Rahmen der Tests sind in den jeweiligen Projektverträgen spezifiziert.

6.2 Integrations- und Funktionsprüfung

Für die von SAP und T-Systems durchzuführende Integrations- und Funktionsprüfung gilt Folgendes:

- 6.2.1 In der Integrations- und Funktionsprüfung wird das Gesamtsystem auf Mangelfreiheit überprüft.
- 6.2.2 Bei Mängeln wird zwischen folgenden drei Mängelklassen unterschieden:
 - (a) Ein betriebsverhindernder Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung unmöglich oder schwerwiegend eingeschränkt ist.
 - (b) Ein betriebsbehindernder Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung erheblich eingeschränkt ist.

- (c) Ein leichter Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung ohne oder mit unwesentlichen Einschränkungen möglich ist.

Ein betriebsbehindernder Mangel liegt auch vor, wenn die leichten Mängel insgesamt zu einer nicht unerheblichen Einschränkung der Nutzung einer vertraglichen Leistung führen.

- 6.2.3 Werden betriebsverhindernde und/oder betriebsbehindernde Mängel festgestellt, ist die Integrations- und Funktionsprüfung durch SAP und T-Systems abzubrechen. Sofern lediglich betriebsbehindernde Mängel festgestellt werden, ist die Funktionsprüfung jedoch nur abzubrechen, wenn deren Fortsetzung aufgrund der Mängel nicht mehr sinnvoll erscheint. SAP und T-Systems teilen dem Auftraggeber nach Abschluss oder Abbruch der Funktionsprüfung bei der Integrations- und Funktionsprüfung festgestellte Mängel entsprechend der vereinbarten Mängelklassifizierung mit.
- 6.2.4 Falls die Integrations- und Funktionsprüfung gemäß vorstehender Ziffer 6.2.3 abgebrochen wird, sind SAP und T-Systems verpflichtet, die Mängel innerhalb einer angemessenen Frist zu beseitigen (in ihrem jeweiligen Leistungsbereich). Nach deren Beseitigung haben SAP und T-Systems führen SAP und T-Systems erneut die Integrations- und Funktionsprüfung erneut durch.
- 6.2.5 Ziffer 6.2.4 gilt auch, wenn die Funktionsprüfung trotz betriebsverhindernder Mängel und/oder betriebsbehindernder Mängel vollständig durchgeführt wird.
- 6.2.6 SAP und T-Systems erklären nach Abschluss der Integrations- und Funktionsprüfung die Betriebsbereitschaft des Gesamtsystems, wenn das Gesamtsystem lediglich leichte Mängel aufweist und diese in ihrer Summe auch nicht als betriebsbehindernde Mängel gelten. Festgestellte Mängel werden in der Erklärung als Mängel festgehalten und von SAP und T-Systems in ihren jeweiligen Leistungsbereichen und nach Maßgabe der jeweiligen Projektverträge unverzüglich beseitigt, soweit nicht eine Frist für die Beseitigung vereinbart ist.

6.3 Freigabe zur Aufnahme des Wirkbetriebs

- 6.3.1 SAP und T-Systems stellen dem Auftraggeber das betriebsbereite Gesamtsystem zur Freigabe zur Aufnahme des Wirkbetriebs bereit, wenn folgende Voraussetzungen erfüllt sind:
- (a) Der Auftraggeber hat erklärt, dass die Einbindung des BSI in die Entwicklung des Gesamtsystems und seiner Komponenten ohne die Feststellung wesentlicher Beanstandungen abgeschlossen ist; die Erklärung darf vom Auftraggeber nicht unbillig verweigert oder verzögert werden.
- (b) Der Auftraggeber hat erklärt, dass die Einbindung des BfDI in die Entwicklung des Gesamtsystems und seiner Komponenten ohne die Feststellung wesentlicher Beanstandungen abgeschlossen ist; die Erklärung darf vom Auftraggeber nicht unbillig verweigert oder verzögert werden.

- (c) Die Übergabe der Dokumentation an den Auftraggeber ist erfolgt.
 - (d) Die in Ziffer 6.1 aufgeführten Tests wurden erfolgreich abgeschlossen, die Testergebnisse liegen dem Auftraggeber vor und es wurden allenfalls leichte Mängel (die auch in ihrer Gesamtheit keinen betriebsbehindernden Mangel darstellen) oder unwesentliche Sicherheitsrisiken identifiziert.
 - (e) Die schriftliche Erklärung von SAP und T-Systems, dass die Integrations- und Funktionsprüfung des Gesamtsystems erfolgreich abgeschlossen wurde und das Gesamtsystem betriebsbereit ist, liegt vor. Das Protokoll der Integrations- und Funktionsprüfung ist der Erklärung beizufügen. Die Erklärung gilt als Betriebsbereitschaftserklärung der T-Systems nach dem T-Systems-Vertrag und als Erklärung der Bereitstellung zur Abnahme der Features nach dem SAP-Vertrag.
- 6.3.2 Der Auftraggeber kann auf einzelne dieser Voraussetzungen für die Demonstration der Betriebsbereitschaft verzichten, insbesondere auch auf die Übergabe einzelner Teile der Dokumentation in finaler Fassung zu den in Anlage 4 genannten Terminen. Dies entbindet die Industriepartner nicht von der Verpflichtung, diese Voraussetzungen herbeizuführen.
- 6.3.3 Nach Vorliegen sämtlicher Voraussetzungen gemäß Ziffer 6.3.1 (oder Verzicht hierauf) und betriebsbereiter Bereitstellung des Gesamtsystems durch SAP und T-Systems erklärt der Auftraggeber innerhalb von zwei (2) Werktagen die Freigabe zur Aufnahme des Wirkbetriebs ("Go-Live-Freigabe"). Die Go-Live-Freigabe hat förmlich zu erfolgen.
- 6.3.4 Die Go-Live-Freigabe gilt in Bezug auf den T-Systems-Vertrag als Freigabe zur Aufnahme des Wirkbetriebs.
- 6.3.5 In Bezug auf SAP stellt die Go-Live-Freigabe eine Abnahme dar; sofern Teile der Dokumentation dem Auftraggeber nicht in finaler Fassung zu den in Anlage 4 genannten Terminen zur Verfügung gestellt wurden oder erst nach Go-Live-Freigabe zur Verfügung zu stellen sind, stellt die Go-Live-Freigabe lediglich eine Teilabnahme der rechtzeitig zur Verfügung gestellten Teile der Leistungen von SAP dar; im Übrigen erfolgt die Abnahme jeweils binnen angemessener Frist nach Bereitstellung der weiteren Teile der Dokumentation. Rechte wegen der in den Testergebnissen festgehaltenen Mängel muss sich der Auftraggeber nicht gesondert vorbehalten.
- 6.3.6 Der Auftraggeber erklärt die Go-Live-Freigabe nur, wenn das Gesamtsystem lediglich leichte Mängel aufweist und diese in ihrer Summe auch nicht als betriebsbehindernde Mängel gelten. Festgestellte Mängel werden in der Go-Live-Freigabe als Mängel festgehalten und von SAP und T-Systems in ihren jeweiligen Leistungsbereichen und nach Maßgabe der jeweiligen Projektverträge unverzüglich beseitigt, soweit nicht eine Frist für die Beseitigung vereinbart ist.
- 6.3.7 Die T-Systems nimmt den Wirkbetrieb des Gesamtsystems innerhalb von einem (1) Werktag nach Go-Live-Freigabe auf.

7. CHANGE REQUEST-VERFAHREN

Die Parteien vereinbaren das nachstehende Verfahren für Änderungen des Leistungsumfangs des Gesamtsystems oder einzelner Komponenten hiervon nach Vertragsschluss ("Change Request-Verfahren"):

7.1 Änderungsverlangen des Auftraggebers

7.1.1 Der Auftraggeber kann nach Vertragsschluss jederzeit Änderungen des Leistungsumfangs des Gesamtsystems im Rahmen der Leistungsfähigkeit von SAP und T-Systems verlangen, es sei denn, dies ist für SAP oder T-Systems unzumutbar.

7.1.2 SAP und T-Systems haben das Änderungsverlangen des Auftraggebers für ihren jeweiligen Leistungsbereich zu prüfen und werden dem Auftraggeber in angemessener Frist, insbesondere unter Berücksichtigung von Art und Umfang des Änderungsverlangens mitteilen, ob es zumutbar und falls nicht, warum es unzumutbar ist.

7.1.3 Hat das zumutbare Änderungsverlangen keinen Einfluss auf die vereinbarte Vergütung oder Termine, haben SAP und T-Systems in ihrem jeweiligen Leistungsbereich und in gegenseitiger Abstimmung unverzüglich mit der Umsetzung des Änderungsverlangens zu beginnen und dies dem Auftraggeber mitzuteilen.

7.1.4 Hat das zumutbare Änderungsverlangen Einfluss auf die vereinbarte Vergütung oder Termine, werden SAP und T-Systems für ihren jeweiligen Leistungsbereich jeweils ein Realisierungsangebot unter Angabe von Terminen und den Auswirkungen auf die vereinbarte Vergütung unterbreiten. Der Auftraggeber wird die Realisierungsangebote in angemessener Frist annehmen oder ablehnen.

7.1.5 Bedarf die Erstellung des Realisierungsangebotes einer umfangreichen technischen Planung, können SAP und/oder T-Systems dieses von der Zahlung einer angemessenen Vergütung abhängig machen. SAP und/oder T-Systems werden in diesem Fall ein entsprechendes Planungsangebot mit Angabe der Vergütung unterbreiten. Der Auftraggeber wird die Planungsangebote in angemessener Frist annehmen oder ablehnen.

■ Kommt eine Vereinbarung über die Änderung der Leistung zustande, ist der jeweilige Projektvertrag, insbesondere die Leistungsbeschreibung, entsprechend anzupassen. Kommt keine Vereinbarung zustande, werden die Arbeiten auf der Grundlage der geltenden Projektverträge weitergeführt. ■

7.2 Änderungsvorschlag von SAP und/oder T-Systemen

7.2.1 SAP und T-Systemen können gemeinsam oder jeweils einzeln Änderungen des Leistungsumfangs des Gesamtsystems vorschlagen. In dem Änderungsverlangen sind anzugeben:

- (a) Art und Umfang der vorgeschlagenen Änderung.
- (b) Grund des Vorschlags und Folgen für den Fall, dass der Vorschlag nicht angenommen wird.
- (c) Auswirkungen des Vorschlags auf Vergütung und Termin- und Leistungspläne.
- (d) Sofern nur SAP oder T-Systemen einzeln den Vorschlag unterbreiten: erwartete Auswirkungen des Vorschlags in Bezug auf den Leistungsbereich des jeweils anderen einschließlich einer Darstellung des erwarteten Änderungsbedarfs.

7.2.2 Sofern der Änderungsvorschlag nur von SAP oder T-Systemen einzeln unterbreitet wird, ist der jeweils andere verpflichtet, binnen angemessener Frist von in der Regel nicht mehr als zehn (10) Werktagen zu dem Vorschlag gegenüber dem Vorschlagenden und gegenüber dem Auftraggeber Stellung zu nehmen und insbesondere Auswirkungen des Vorschlags auf seinen Leistungsbereich darzulegen, insbesondere hinsichtlich Vergütung sowie Termin- und Leistungspläne. Ziffer 7.1 gilt entsprechend.

7.2.3 Kommt eine Vereinbarung über die Änderung der Leistung zustande, ist der jeweilige Projektvertrag, insbesondere die Leistungsbeschreibung, entsprechend anzupassen. Kommt keine Vereinbarung zustande, werden die Arbeiten auf der Grundlage der geltenden Projektverträge weitergeführt.

7.3 Allgemeine Bestimmungen

7.3.1 Das Änderungsverfahren ist auf einem Formular gemäß Anlage 6 zu dokumentieren, soweit nichts anderes vereinbart ist.

7.3.2 Auf berechnete Vertraulichkeitsinteressen von SAP und T-Systemen ist bei der Durchführung des Change Request-Verfahrens und beim Austausch von Informationen zwischen den Parteien Rücksicht zu nehmen. SAP und T-Systemen werden vertrauliche Informationen entsprechend kennzeichnen.

8. HAFTUNG

8.1 Haftung der Industriepartner gegenüber dem Auftraggeber und Dritten

Eine gesamtschuldnerische Haftung der Industriepartner gegenüber dem Auftraggeber und Dritten ist nicht beabsichtigt. Jeder Industriepartner achtet in seiner

Vertragsbeziehung mit dem Auftraggeber und in seiner sonstigen Außendarstellung darauf, dass nicht der Eindruck einer gesamtschuldnerischen Haftung erweckt wird und ist insbesondere nicht befugt, im Namen des jeweils anderen Industriepartner oder für beide Industriepartner gemeinsam Erklärungen gegenüber Dritten abzugeben und wird dies unterlassen.

8.2 Haftung der Industriepartner untereinander ohne Drittbezug

Für von einem Industriepartner beim anderen Industriepartner verursachte Schäden ohne Bezug zum Auftraggeber oder Dritten haften die Industriepartner wie folgt.

8.2.1 Für vorsätzlich oder grob fahrlässig verursachte Schäden und Aufwendungen sowie bei Verletzung des Lebens, des Körpers oder der Gesundheit und bei einer Haftung nach dem Produkthaftungsgesetz haften die Industriepartner einander im Rahmen der gesetzlichen Bestimmungen.

8.2.2 Für leicht fahrlässig verursachte Schäden und Aufwendungen haften die Industriepartner einander bis zu einem Betrag von maximal [REDACTED] pro Schadensfall und Kalenderjahr. Die Haftung für entgangenen Gewinn ist ausgeschlossen.

8.3 Erstreckung der Haftungsbegrenzung im Verhältnis zum Auftraggeber

Ziffer 10 der AGB für Services in Verbindung mit Ziffer 7.8 der Order Form (die jeweils Bestandteile des SAP-Vertrags sind) und Ziffer 9 des T-Systems-Vertrags gelten im Verhältnis der jeweiligen Industriepartner zum Auftraggeber auch für Pflichtverletzungen unter dieser Abstimmungsvereinbarung.

9. NUTZUNGSRECHTE

9.1 Keine direkte Einräumung von Nutzungsrechten

Die Industriepartner gehen davon aus, dass für die Leistungserbringung des jeweils anderen Industriepartners keine Einräumung von Nutzungsrechten erforderlich ist. Es ist daher nicht vorgesehen, dem jeweils anderen Industriepartner Nutzungsrechte einzuräumen. Dessen ungeachtet ist jeder Industriepartner unter Beachtung der Regelungen zur Geheimhaltung gemäß Ziff. 9 berechtigt, im Rahmen dieses Vertrags überlassene Informationen für die Entwicklung und den Betrieb der Anti-Corona-App zu nutzen.

9.2 Nutzungsrechte unter Projektverträgen

Die Einräumung von Nutzungsrechten gegenüber dem Auftraggeber wird in den jeweiligen Projektverträgen der SAP beziehungsweise der T-Systems mit dem Auftraggeber geregelt und bleibt von Ziffer 9.1 unberührt.

10. GEHEIMHALTUNG

10.1 Nutzung vertraulicher Informationen

Die zwischen den Parteien im Zusammenhang mit den Projektverträgen und dieser Abstimmungsvereinbarung ausgetauschten Geschäftsgeheimnisse sowie sonstige

Unterlagen, Kenntnisse, Erfahrungen und Informationen, die bei vernünftiger Betrachtungsweise als vertraulich einzustufen sind (nachfolgend "vertrauliche Informationen" genannt) dürfen ausschließlich für die Zwecke der Projektverträge verwendet werden.

10.2 Geheimhaltungsmaßnahmen

Für die vertraulichen Informationen sind angemessene Geheimhaltungsmaßnahmen durch die Parteien zu treffen. Die Parteien verpflichten sich, die ausgetauschten vertraulichen Informationen Dritten gegenüber geheim zu halten. Als Dritte gelten nicht die jeweils verbundenen Unternehmen gemäß §§ 15 ff. AktG der jeweiligen Partei sowie für den Auftraggeber Stellen und Organe des Bundes und der Bundesverwaltung, soweit an diese im Zusammenhang mit der Durchführung dieses Vertrages vertrauliche Informationen übergeben werden müssen und, im Fall von verbundenen Unternehmen, diese ihrerseits generell oder spezifisch zur Geheimhaltung verpflichtet sind sowie entsprechend verpflichtete Subunternehmer der jeweiligen Partei.

10.3 Ausnahmen

Die Geheimhaltungsverpflichtung gilt nicht, solange und soweit die Informationen:

- 10.3.1 dem Empfänger bereits ohne Geheimhaltungsverpflichtung bekannt waren oder
- 10.3.2 allgemein bekannt sind oder werden, ohne dass dies der Empfänger zu vertreten hat oder
- 10.3.3 dem Empfänger von einem Dritten ohne Geheimhaltungsverpflichtung mitgeteilt bzw. überlassen werden oder
- 10.3.4 vom Empfänger nachweislich unabhängig entwickelt worden sind oder
- 10.3.5 von der überlassenden Partei zur Bekanntmachung schriftlich freigegeben worden sind oder
- 10.3.6 der Empfänger aufgrund von gesetzlichen Vorschriften gegenüber Behörden oder Dritten mitzuteilen verpflichtet ist.

10.4 Entfall

Die Verpflichtung zur Geheimhaltung und Nichtverwertung entfällt, soweit die Weitergabe von vertraulichen Informationen im Projekt Corona Warn App erforderlich ist, gegenüber dem Bundesministerium für Gesundheit, dem RKI, dem BSI, dem BfDI, der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. ("FH") sowie weiteren nach den Regelungen in Anlage 3 in die Projektorganisation einbezogenen Dritten.

10.5 Dauer der Geheimhaltungsverpflichtung

Die Geheimhaltungsverpflichtung endet 10 (zehn) Jahre nach der Beendigung dieser Abstimmungsvereinbarung.

11. DATENSCHUTZ

Die jeweilige Partei hält bei der Leistungserbringung jeweils die auf sie anwendbaren Datenschutzgesetze ein.

Soweit eine Partei für eine andere Partei personenbezogene Daten im Auftrag verarbeitet, werden die jeweiligen Parteien vor Beginn der Verarbeitung eine Vereinbarung zur Auftragsverarbeitung abschließen.

12. ALLGEMEINE BESTIMMUNGEN

12.1 Keine gesonderte Vergütung / Kostentragung

12.1.1 Die Leistungen von SAP und T-Systems unter dieser Abstimmungsvereinbarung sind mit der Vergütung unter dem SAP-Vertrag bzw. dem T-Systems-Vertrag vollständig abgegolten. Diese Abstimmungsvereinbarung begründet keine Ansprüche der Industriepartner auf Zahlung einer Vergütung oder auf Ersatz von Aufwendungen, sofern nicht ausdrücklich etwas anderes geregelt ist.

12.1.2 Jede Partei trägt die jeweiligen ihr entstehenden Kosten im Rahmen dieser Abstimmungsvereinbarung selbst.

12.2 Laufzeit / Beendigung

12.2.1 Diese Abstimmungsvereinbarung endet im Verhältnis zu SAP mit Beendigung des SAP-Vertrags und im Verhältnis zur T-Systems mit Beendigung des T-Systems-Vertrags (jeweils gleich aus welchem Rechtsgrund), ohne dass es einer Kündigung bedarf. Das Recht zur ordentlichen isolierten Kündigung dieser Abstimmungsvereinbarung ist ausgeschlossen; Kündigungsrechte unter den übrigen Projektverträgen bleiben hiervon unberührt. Das gesetzliche Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Die Beendigung dieser Abstimmungsvereinbarung (gleich aus welchem Rechtsgrund) lässt die übrigen Projektverträge unberührt; die Bestimmungen in Ziffern 3 bis 7 gelten in diesem Fall im Verhältnis zu SAP als Bestandteil des SAP-Vertrags und im Verhältnis zur T-Systems als Bestandteil des T-Systems-Vertrags fort.

12.2.2 SAP und T-Systems verpflichten sich jeweils, eine dieser Abstimmungsvereinbarung im Wesentlichen entsprechende Vereinbarung mit einem Dritten abzuschließen, der SAP bzw. T-Systems als Industriepartner im jeweiligen Leistungsbereich nachfolgt.

12.3 Schlussbestimmungen

12.3.1 Die Anlagen sind Bestandteil dieser Abstimmungsvereinbarung.

12.3.2 Bei Widersprüchen geht diese Abstimmungsvereinbarung den übrigen Projektverträgen vor.

12.3.3 Bezugnahmen auf die Projektverträge sind Bezugnahmen auf die jeweils gültige Fassung.

- 12.3.4 Änderungen und Ergänzungen dieser Abstimmungsvereinbarung sowie der Verzicht auf sich aus dieser Abstimmungsvereinbarung ergebende Rechte bedürfen zu ihrer Wirksamkeit der Schriftform (jedoch unter Einschluss einer telekommunikativen Übermittlung). Dies gilt auch für die Änderung oder Aufhebung dieser Schriftformklausel.
- 12.3.5 Ausschließlicher Gerichtsstand für alle sich aus oder im Zusammenhang mit dieser Abstimmungsvereinbarung oder über ihre Wirksamkeit ergebenden Streitigkeiten (einschließlich solcher über deliktsrechtliche Ansprüche) zwischen den Parteien, für die kein anderer, ausschließlicher Gerichtsstand besteht, ist Bonn. Soweit die vertragliche Bestimmung des Erfüllungsortes gesetzlich zulässig ist, ist Erfüllungsort für alle sich aus der Abstimmungsvereinbarung ergebenden Verpflichtungen der Sitz des Bundesministeriums für Gesundheit bzw. nach Übertragung der Durchführung der Projektverträge auf das RKI der Sitz des RKI in Berlin. Der Erfüllungsort gemäß SAP-Vertrag und gemäß T-Systems-Vertrag bleibt unberührt.
- 12.3.6 Dieser Vertrag unterliegt deutschem Recht unter Ausschluss des UN-Kaufrechts.
- 12.3.7 Sollte eine Bestimmung dieser Abstimmungsvereinbarung ganz oder teilweise nichtig sein oder werden oder sollte sich eine Lücke in diesem Vertrag herausstellen, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. In diesem Fall gilt mit Rückwirkung diejenige wirksame und durchführbare Regelung als vereinbart, die rechtlich und wirtschaftlich dem am nächsten kommt, was die Parteien gewollt haben oder nach dem Sinn und Zweck dieser Abstimmungsvereinbarung gewollt hätten, wenn sie diesen Punkt beim Abschluss des Vertrags bedacht hätten. Beruht die Nichtigkeit einer Bestimmung auf einem darin festgelegten Maß der Leistung oder der Zeit (Frist oder Termin), so gilt die Bestimmung mit einem dem ursprünglichen Maß am nächsten kommenden rechtlich zulässigen Maß als vereinbart. Es ist der ausdrückliche Wille der Parteien, dass diese salvatorische Klausel nicht lediglich die Beweislast umkehrt, sondern § 139 BGB insgesamt abbedungen wird, so dass dieser Vertrag trotz einer nichtigen Bestimmung oder einer Lücke aufrechterhalten bleibt.

* * *

Projekt Corona Warn App – Abstimmungsvereinbarung

- Unterschriftenseite -

Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit:

Dr. Thomas Steffen

Name, Funktion

Dln. 11.06.2020

Ort, Datum

i.V. J.C.H.

Unterschrift

SAP Deutschland SE & Co. KG

ppa. Kirstin Graichen

Name, Funktion

ppa. Gabriele Spiess

Name, Funktion

Jun 9, 2020

Ort, Datum

June 9, 2020

Ort, Datum

Digitally signed by
ppa. Kirstin Graichen
Unterschrift

Digitally signed by
ppa. Gabriele Spiess
Unterschrift

T-Systems International GmbH

Name, Funktion

Name, Funktion

Ort, Datum

Peter Lorenz

Digital unterschrieben von Peter Lorenz
Datum: 2020.06.08 13:18:56
+02'00'

Unterschrift

Ort, Datum

Adel Al-Saleh

Digital unterschrieben von Adel Al-Saleh
Datum: 2020.06.08 18:59:28
+02'00'

Unterschrift

Unterschriftfassung

**ANLAGE 1
SPEZIFIKATIONEN**



Spezifikation

Corona-Warn-App

Dokumentenversion: 1.1 – Endgültige Version
Datum: 5. Juni 2020

Vertraulich

Historie

Version	Datum	Kommentar
1.0	3. Juni 2020	Initiale Version
1.1	5. Juni 2020	Kapitel 3 Projektumfang: Update auf Basis des zugrundeliegenden GitHub-Dokuments <i>Scoping Dokument</i> Kapitel 4 Architektur: Referenz auf das GitHub-Dokument <i>Solution Architecture</i>

Inhalt

1	INFORMATIONEN ZUM DOKUMENT	6
1.1	Glossar	6
2	GESCHÄFTLICHER KONTEXT	6
2.1	Einleitung	6
2.2	User Journey	7
2.2.1	Beschreibung der Nutzungsprofile (Stakeholder)	7
2.2.2	User Journey	8
3	PROJEKTUMFANG	10
3.1	Abgrenzung der Leistungen der Parteien	10
3.1.1	Übersicht zur Leistungsabgrenzung	10
3.1.2	Aufgaben und Leistungsumfang der SAP	10
3.1.3	Aufgaben und Leistungsumfang der T-Systems	11
3.2	Abgrenzung zum Scoping Document auf GitHub	12
3.3	Übersicht der Epics	13
3.3.1	Prozessphasen der Nutzung	13
3.3.2	Supportprozesse	14
3.4	Übersicht der User Stories	18
3.4.1	Anbahnung und Installation (Onboarding-Prozess)	18
3.4.2	Informationen und Instruktionen zur Nutzung der App	18
3.4.3	Nutzung im Regelprozess	19
3.4.4	Kontaktfall (Begegnung mit infizierter Person)	21
3.4.5	Covid-19-Testergebnismeldung	22
3.4.6	Auslösen einer Warnung	23
3.4.7	Parametrierung	26
3.4.8	Technische Unterstützung	26
3.4.9	Barrierefreiheit	28
3.4.10	Content Management	27
4	ARCHITEKTUR	28

Abbildungsverzeichnis

Abbildung 1: User Journey.....	8
Abbildung 2: Leistungsbereiche der Industriepartner.....	10

1 Informationen zum Dokument

Diese Spezifikation ist die Grundlage für die Entwicklungen, die durch SAP vorgenommen werden. Sie beschreibt den Leistungsumfang, der durch SAP im Rahmen des Projektes bereitgestellt wird.

1.1 Glossar

Das Glossar zur Corona-Warn-App ist öffentlich auf GitHub einsehbar:

<https://github.com/corona-warn-app/cwa-documentation/blob/master/glossary.md>

2 Geschäftlicher Kontext

Hinweis

Dieses Kapitel stellt allgemeine Hintergrundinformationen zur Verfügung. Konkrete Anforderungen an die Software sind in Kapitel 3 Projektumfang spezifiziert.

2.1 Einleitung

Ziel der Corona-Warn-App ist es, SARS-CoV-2-Infektionsketten schnellstmöglich zu erkennen und zu durchbrechen. Personen sollen zuverlässig und schnell über Begegnungen mit anderen infizierten Personen und damit mögliche Übertragungen des Virus informiert werden, damit sie sich freiwillig isolieren können, um damit zu einer Eindämmung der SARS-CoV-2-Pandemie beizutragen.

Dieses Dokument beschreibt die funktionalen Anforderungen an die Gestaltung der App aus einer fachlichen und prozessualen Sicht. Die Beschreibung ist in der aktuellen Version inhaltlich auf das erste Release begrenzt und eine initiale Version.

In der Gesamtplanung ist die Veröffentlichung weiterer Dokumente aus der Entwicklung vorgesehen, um frühzeitig Rückmeldungen zu erhalten und gegebenenfalls aufzunehmen. Nachfolgend werden zunächst das Release-Architektur-Dokument sowie der Backend-Source-Code alpha verfügbar gemacht.

Die Definition und Gliederung der Anforderungen folgen einer personenzentrierten Methodik. Dabei erfolgt die Gestaltung des gesamten Prozessablaufs aus Sicht derjenigen, welche die App nutzen, bzw. der im Prozess eingebundenen Stakeholder. Das Ziel ist es, die Bedürfnisse aller genannten Beteiligten so abzubilden, dass eine hohe Akzeptanz erreicht wird und die jeweiligen Funktionen intuitiv bedienbar sind.

Anhand einer User Journey (Nutzungsreise) sind die Interaktionspunkte und das Erlebnis während der Nutzung aufgezeigt. Die daraus entstehenden Anforderungen werden sogenannten Epics (Beschreibung einer Anforderung auf einer hohen Abstraktionsebene) zugeordnet. Die Epics beschreiben die einzelnen Kontakt-Ereignisse sowie übergreifende Funktionalitäten im gesamten Prozess, die für die Nutzung und Akzeptanz der App erforderlich sind. Aus den Epics heraus werden die detaillierten Anforderungen in Form sogenannter User Stories (eine in Alltagssprache formulierte Software-Anforderung) abgeleitet. Die einzelnen Anforderungen werden so strukturiert in den Entwicklungsprozess gebracht.

2.2 User Journey

2.2.1 Beschreibung der Nutzungsprofile (Stakeholder)

Folgende wesentliche Nutzungsprofile bzw. Stakeholder sind in die User Journey bzw. in den Gesamtprozess eingebunden und in ihrer Rolle beschrieben:

App-Bedienung

Alle Personen, welche die App benutzen: Werden über mögliche Begegnungen mit infizierten Personen informiert, verifizieren eigene Testergebnisse bzw. warnen dann alle Personen, denen sie begegnet sind, freiwillig und pseudonym.

Hotlines

Unterstützen Personen bei der Bedienung der App in der Beantwortung von Fragestellungen zur Nutzung der App, zur Technik sowie zum Datenschutz und geben auf Nachfrage verhaltensbezogene Informationen sowie weitere Informationmöglichkeiten im Kontakt- bzw. Infektionsfall weiter. Unterstützen bei Verifikation und Freilegung von Testergebnissen in der App für infizierte Personen und können diesen die Kontaktaufnahme mit dem zuständigen Gesundheitsamt empfehlen.

Robert Koch-Institut (RKI)

Stellt epidemiologische Informationen und Handlungsempfehlungen für die Bedienung der App zur Verfügung (Content). Bestimmt die Parameter für die Messung der Kontakte (im Rahmen der technischen Möglichkeiten durch die API).

2.2.2 User Journey

Die Nutzung der App wird aufgrund von nacheinander stattfindenden Kontakt-Ereignissen und Interaktionen von Personen in verschiedene Phasen eingeteilt. Zu jeder Phase sind den Personen Motivationen oder Anforderungen zugeordnet, die ihre Erwartungen an die Funktionsweise erfüllen und intuitiv durch den Prozess leiten.

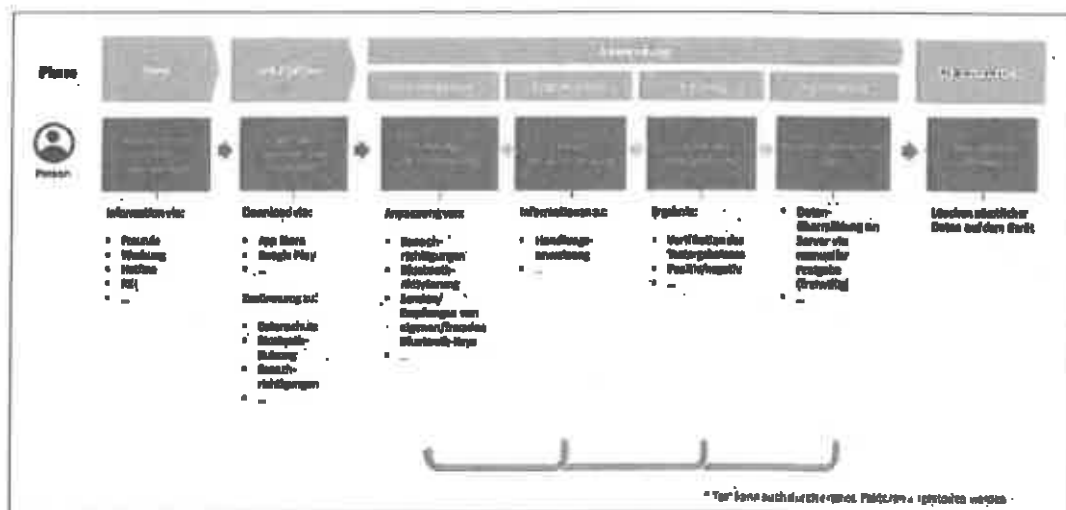


Abbildung 1: User Journey

Phase Idee

In dieser Phase entscheidet eine Person, sich über die App zu informieren. Das kann über unterschiedliche Quellen erfolgen. In dieser Phase haben die Personen ggf. verschiedene Fragestellungen zur Nutzung der App (Anwendung, Datenschutz, Barrierefreiheit etc.). Diese sollen bereits vor dem Download beantwortet werden können (Hotline, Informationen auf Internetseiten des RKI und des BMG, App Store/Google Play Store).

Phase Installation

Eine Person entscheidet sich zum Download der App (App Store/Google Play Store) und wird nach der technischen Installation beim erstmaligen Öffnen der App durch eine Einführung begleitet. In der Einführungsphase erhält die Person eine Übersicht über die Funktionsweise, Nutzungsbedingungen und Datenschutzbestimmungen sowie erforderliche Einwilligungen, Einstellungen und Benachrichtigungen.

Phase Anwendung

Die Phase der Anwendung ist in vier weitere Bereiche unterteilt, in welchen die Person unterschiedliche Bedürfnisse hat.

1. Hintergrund

Im Ruhezustand (Idle Mode) des Mobiltelefons läuft die Anwendung im Hintergrund und speichert für die Person automatisiert und verschlüsselt die in der Nähe befindlichen Pseudo-IDs anderer Personen anhand definierter Parameter über Entfernung und Dauer des Kontaktes. In regelmäßigen Abständen holt sich die App vom Server eine Liste der Pseudo-IDs der sich freiwillig infiziert gemeldeten Personen und vergleicht diese mit den gespeicherten Pseudo-IDs im Gerät, um einen möglichen Kontakt zu ermitteln.

2. Kontaktfall

Im festgestellten Kontaktfall zu infizierten Personen erhält die Person jeweils eine Benachrichtigung und verhaltensbezogene Empfehlungen. Hier kann zum Beispiel die Kontaktaufnahme mit ärztlichem Fachpersonal, mit dem zuständigen Gesundheitsamt und/oder die freiwillige häusliche Isolation empfohlen werden.

3. Testing

Im Fall eines durchgeführten Tests auf eine SARS-CoV-2-Infektion kann die Person über die App den digitalen Testinformationsprozess starten und damit über das ermittelte Testergebnis benachrichtigt werden.

4. Infektfall

Im Fall eines positiven SARS-CoV-2-Befunds kann eine Person freiwillig die in der App gespeicherten eigenen pseudonymen Warn-IDs veröffentlichen, damit andere Personen, die die App nutzen, auf ihrem eigenen Smartphone abgleichen können, ob sie mit der infizierten Person in Kontakt standen.

Phase Deinstallation

Eine Person kann die App jederzeit deinstallieren. Alle in der App gespeicherten Daten werden vollständig gelöscht.

3 Projektumfang

3.1 Abgrenzung der Leistungen der Parteien

3.1.1 Übersicht zur Leistungsabgrenzung

SAP und T-Systems wollen auf Basis jeweils gesonderter Verträge mit dem Bundesministerium für Gesundheit (BMG) eine Tracing-App entwickeln und betreiben, um Kontaktpersonen von Corona-Infizierten warnen zu können („Corona-Warn-App“). SAP und T-Systems erbringen hierzu gesonderte Leistungen gegenüber dem BMG. In der nachfolgenden Darstellung sind die Leistungsbereiche der Industriepartner schematisch dargestellt:

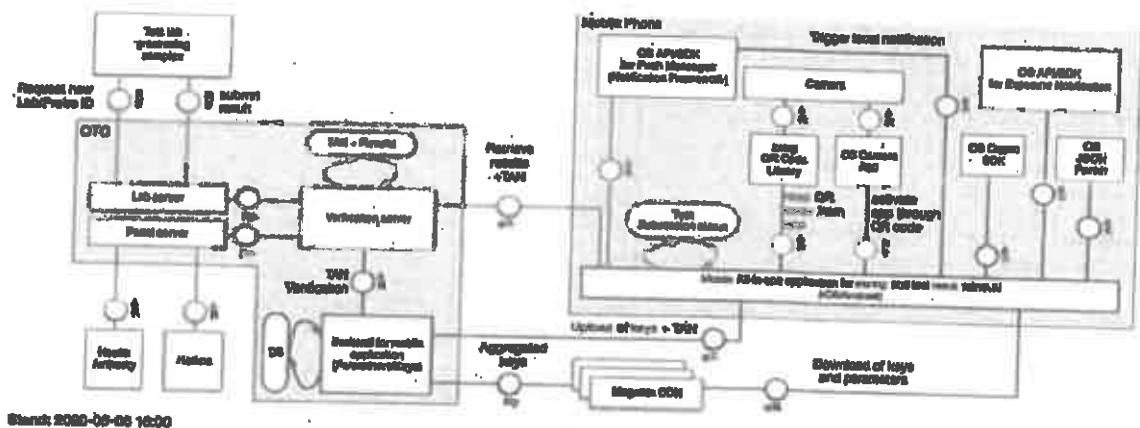


Abbildung 2: Leistungsbereiche der Industriepartner

3.1.2 Aufgaben und Leistungsumfang der SAP

Die Leistungen der SAP umfassen:

- Design und Entwicklung der Corona-Warn-App (iOS und Android); basierend auf einem neuen SDK, das von Apple und Google zur Verfügung gestellt wird und als Exposure Notification Framework bezeichnet wird,
- Entwicklung des Backends zur Entgegennahme von Upload-Anfragen der Clients (Tracing Server); Übergabe von Konfigurationsparametern an die mobilen Anwendungen und Zusammenfassung der Diagnoseschlüssel in Blöcke,
- Publizieren der wesentlichen Projektbestandteile als Open Source auf GitHub.

3.1.3 Aufgaben und Leistungsumfang der T-Systems.

Die Leistungen der T-Systems ergeben sich aus T-Systems-Vertrag. Diese umfassen insbesondere:

- Die Entwicklung und den Betrieb des Verifikationsservers, des Lab Servers sowie des Portal Servers innerhalb des Prozesses zur Verifizierung / Falsifizierung einer gemeldeten Infektion,
- Betrieb des Backends zur Entgegennahme von Upload-Anfragen der Client (Tracing Server),
- Bereitstellung einer Managed „Platform as a Service“ (PaaS),
- Hotline Service.

3.2 Abgrenzung zum Scoping Document auf GitHub

Die nachfolgenden Kapitel entsprechen wortgenau dem deutschen Scoping Document der Corona-Warn-App (Stand: 05.08.2020), welches öffentlich auf GitHub einsehbar ist:

https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/scoping_document.de.md

3.3 Übersicht der Epics

Die Funktionen der App sind in Prozessphasen der Nutzung (mit direktem Bezug zur User Journey) und übergreifende Unterstützungsprozesse unterteilt. Eine Übersicht der Epics ist nachfolgend dargestellt:

3.3.1 Prozessphasen der Nutzung

#	Epic	Beschreibung
1.	Anbahnung und Installation (Onboarding-Prozess)	Sämtliche Prozesse, die insbesondere bei erstmaliger Nutzung der App erfolgen (z.B. Zustimmung Datenschutz, Sprachauswahl)
2	Informationen und Instruktionen zur Nutzung der Applikation	Hilfestellungen zur Nutzung der App (z.B. Anwendungshandbuch, Tutorial) sowie Informationen zum Impressum der App
3	Nutzung im Regelprozess	Funktionen der App im "Idle mode" (z.B. Aktivierung/Deaktivierung, Anpassung von Einstellungen, Überwachung von App-Aktivität)
4	Kontaktfall (Begegnung mit infizierter Person)	Funktionen rund um Kontaktpunkte (z.B. Benachrichtigungen, Handlungsempfehlungen)
5	Covid-19-Testergebnismeldung	Funktionen im Zusammenhang mit der Testergebnismeldung
6	Auslösung einer Warnung	Prozesse zur Auslösung einer Warnung im Falle eines positiven Testergebnisses

3.3.2 Supportprozesse

#	Epic	Beschreibung
7	Parametrisierung	Parameter der Kontaktpunktdefinition
8	Technische Unterstützung	Support-Prozesse (z.B. Hotlines)
9	Barrierefreiheit	Apps von Trägern öffentlicher Gewalt müssen dem Behindertengleichstellungsgesetz (BGG) nach barrierefrei sein (§ 12). Apps sollen von allen Menschen mit Behinderungen bedient werden können.
10	Content-Management	Zur Anpassung und Aktualisierung von Inhalten in der App (Texte, Links, Hotlines etc.)

3.4 Übersicht der User Stories

Die Anforderungen an die Corona-Warn-App, die den fachlichen Umfang der Anwendung definieren, sind nachfolgend in der üblichen Form aus Sicht der nutzenden Personen formuliert, sofern nicht anders angegeben:

„Als <Stakeholder> möchte ich <Handlung durchführen>, um <gewünschtes Ergebnis zu erzielen>.“

Die zugehörigen Akzeptanzkriterien ergänzen die Spezifikation der Anforderungen, indem sie Bedingungen definieren, die die Software erfüllen muss, um die Bedürfnisse der nutzenden Personen zu befriedigen.

3.4.1 Anbahnung und Installation (Onboarding-Prozess)

# User Story ID	User Story	Akzeptanzkriterien
E01.01	Als Person, die die App nutzt, möchte ich beim erstmaligen Start der App eine Einleitung zur Funktionsweise der App erhalten (App-Motivation).	<ol style="list-style-type: none">1. Einführung in die Funktionsweise der App wird bei erstmaligem Start der Applikation angezeigt.2. Einführung in die Funktionsweise der App wird bei weiteren Startvorgängen nicht angezeigt.3. Die erklärenden Inhalte sind in den jeweiligen Funktionsbereichen zur Nutzung vorhanden.

E01.02

Bei der Nutzung der App möchte ich beim erstmaligen Start der App über die Nutzungsbedingungen und Datenschutzbestimmungen (Data Protection Screen) informiert werden und meine Zustimmung geben, um über den Umgang mit meinen Daten innerhalb der Anwendung aufgeklärt zu sein.

1. Mit Nutzung der App akzeptiert die Person die Nutzungsbedingungen und Datenschutzbestimmungen.

2. Die Nutzungsbedingungen sind innerhalb der App einsehbar.

3. Die Abfrage erfolgt nur bei der erstmaligen Nutzung.

E01.03

Als Person, die die App nutzt, möchte ich bei der erstmaligen Nutzung der App gefragt werden, ob ich der Erstellung pseudonymer IDs und deren Aussendung an Geräte in meiner Nähe durch die App zustimme, damit ich über die Funktionsweise der App informiert bin.

1. Eine Bestätigung der Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe durch die App ist Voraussetzung für die Nutzung der entsprechenden Funktionalitäten zur Risiko-Ermittlung.

2. Nach der erstmaligen Nutzung erfolgt die Abfrage nicht.

E01.04

Bei der erstmaligen Nutzung der App möchte ich gefragt werden, ob die App auf die Bluetooth-Funktion des Smartphones zugreifen darf, damit ich die mobiltelefonseitige Nutzung der App kontrollieren kann.

1. Diese User Story ist gleichbedeutend mit E01.03. Die Berechtigung zur Nutzung der Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe beinhaltet die Nutzung von Bluetooth Low Energy (BLE) bereits.

2. Die Einstellungen für die generellen Bluetooth-Funktionalitäten sind nur in den Systemeinstellungen möglich.

E01.05

Bei der erstmaligen Nutzung der App möchte ich gefragt werden, ob die App mir Benachrichtigungen schicken darf, damit in verschiedenen Situationen Push-Notifications ausgegeben werden können.

1. Eine Abfrage zu den Benachrichtigungseinstellungen der App findet vor der erstmaligen Nutzung statt. Es können damit lokale Benachrichtigungen erhalten werden. Echte Push-Notifications von externen Servern werden nicht unterstützt (APNs/GCM).

2. Nach der erstmaligen Nutzung erfolgt die Abfrage nicht.

E01.06

Als Person, die die App nutzt, möchte ich bei der erstmaligen Nutzung der App meine Sprache angezeigt bekommen, damit die Nutzung der App für mich verständlich ist.

1. Erkennung der eingestellten System Sprache wird durchgeführt.

2. Wenn die erkannte System Sprache nicht im Content hinterlegt ist, wird im Default Englisch ausgewählt.

3. In der ersten Version der App ist Mehrsprachigkeit vorgesehen.

E01.07

Als Person, die die App nutzt, möchte ich bereits während des Onboardings Hilfen und Einstellungen zur Barrierefreiheit bekommen, um die App nutzen zu können.

1. Die Barrierefreiheit wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems genutzt.

3.4.2 Informationen und Instruktionen zur Nutzung der App

# User Story ID	User Story	Akzeptanzkriterien
E02.01	Als Person, die die App nutzt, möchte ich Zugriff auf eine FAQ-Liste haben, um mir bei Fragen zur App selbst weiterhelfen zu können.	1. Es wird entweder ein Link auf eine Internetseite mit FAQs zur Verfügung gestellt, oder die Internetseite integriert innerhalb der App dargestellt.
E02.02	Als Person, die die App nutzt, möchte ich Zugriff auf eine Anleitung haben, um die App und ihre Funktionen zu verstehen.	1. Eine entsprechende Erläuterung der verschiedenen Funktionalitäten der App wird bereitgestellt.
E02.03	Als Person, die die App nutzt, möchte ich Zugriff auf ein Erklärvideo haben, um die App und ihre Funktionen zu verstehen.	1. Videos werden nicht in der App eingebettet, können aber beispielsweise über die FAQs zur Verfügung gestellt werden.
E02.04	Als Person, die die App nutzt, möchte ich das Impressum der App einsehen können, um zu sehen, wer für die Entwicklung und Inhalte der App verantwortlich ist.	1. Es gibt ein Untermenü "Impressum". 2. Das Impressum beinhaltet die üblichen Angaben zur Impressumspflicht.
E02.05	Als Person, die die App nutzt, möchte ich Nutzungsbedingungen und Datenschutzinformationen jederzeit einsehen können.	1. Die App bietet einfachen Zugriff auf Nutzungsbedingungen und Datenschutzinformationen.

E02.06	<p>Bei der Nutzung der App möchte ich die verschiedenen Hotlines zu technischen, datenschutzbezogenen, gesundheitsbezogenen und psychologischen Fragestellungen sowie zur Verifikation eines Testergebnisses angezeigt bekommen, damit ich weitere Informationen oder Antworten auf Fragen erhalte.</p>	<ol style="list-style-type: none"> 1. Die App bietet einen Zugriff auf eine technische Hotline und eine Hotline zur Erlangung einer Telefon-TAN. 2. Die zeitliche Erreichbarkeit der Hotlines (z.B. 24/7) wird angezeigt. 3. Telefonnummern können direkt aus der App gewählt werden.
--------	---	--

3.4.3 Nutzung im Regelprozess

# User Story ID	User Story	Akzeptanzkriterien
E03.01	<p>Als Person, die die App nutzt, möchte ich die App aktivieren und deaktivieren können, um die Funktion ein- und auszuschalten.</p>	<ol style="list-style-type: none"> 1. Die Funktionalität zur Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe kann ein- und ausgeschaltet werden. 2. Die Konsequenzen des Ein-/Ausschaltens werden erklärt.

E03.02

Als Person, die die App nutzt, möchte ich die App in den Auslieferungszustand zurücksetzen können, damit ich sie neu konfigurieren kann.

1. Die App kann über eine Einstellung in den Auslieferungszustand zurückgesetzt werden. Die gespeicherten Traces müssen über die Systeminstellungen gelöscht werden.

1. Ein Menü zu App-Einstellungen kann durch die nutzende Person aufgerufen werden.

2. Die Benachrichtigungen können ein- und ausgeschaltet werden.

E03.03

Bei der Nutzung der App möchte ich die Applikationseinstellungen (Zugriffrechte, z.B. Benachrichtigungen) in einem Menü anpassen können, um Funktion und Zugriffe der App verwalten zu können.

3. Der Zugriff auf die Funktionalität zur Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe kann ein- und ausgeschaltet werden.

4. Vor der Deaktivierung der Zugriffrechte erhalte ich Informationen darüber, welche Funktionen der App dadurch nicht mehr (vollumfänglich) funktionieren.

3.4.4 Kontaktfall (Begegnung mit infizierter Person)

# User Story ID	User Story	Akzeptanzkriterien
E04.01	Bei der Nutzung der App möchte ich informiert werden, wenn eine Person, zu der ich Kontakt hatte, sich als infiziert gemeldet hat. Damit kann ich geeignete Maßnahmen treffen, um die Verbreitung des Virus zu stoppen.	<ol style="list-style-type: none">1. In Abhängigkeit der Benachrichtigungseinstellung schickt die App eine Benachrichtigung an die nutzende Person.2. Bei einer Änderung der Risikoeinschätzung für die nutzende Person informiert die Benachrichtigung die nutzende Person über Neuigkeiten in der App. Die tatsächlich geänderte Risikoeinschätzung wird erst innerhalb der App angezeigt.
E04.02	Als Person, die die App nutzt, möchte ich im Kontaktfall Handlungsempfehlungen durch die App bekommen, um mein Verhalten an die Empfehlungen des RKI anzupassen	<ol style="list-style-type: none">1. Die Benachrichtigung führt die nutzende Person zur App. Handlungsempfehlungen des RKI sind in der App statisch hinterlegt.

3.4.5 Covid-19-Testergebnismeldung

# User Story ID	User Story	Akzeptanzkriterien
E05.01	Als RKI möchte ich, dass ausschließlich positiv getestete Personen einmalig eine Warnung auslösen können, um Missbrauch zu vermeiden.	<ol style="list-style-type: none">1. Nur positive Tests können eine Warnung auslösen. Der Verifikationsserver und die Hotline zum Telefon-TAN Verfahren stellen dies sicher.2. Für jeden Test kann nur einmal eine Warnung ausgelöst werden.
E05.02	Bei der Nutzung der App möchte ich im Falle eines positiven Testergebnisses Informationen über die Erkrankung und nötige nächste Schritte bekommen, um mein Verhalten an die Handlungsempfehlungen des RKI anpassen zu können.	<ol style="list-style-type: none">1. Eine Benachrichtigung informiert lediglich über Neuigkeiten in der App. Das Testergebnis selbst kann nur in der App eingesehen werden.2. In der App wird ein Infotext mit definiertem Inhalt angezeigt (z.B. Informationen zum Ausgang des Testergebnisses, Informationen über erforderliche Maßnahmen, eine Hotline-Nummer).

3.4.6 Auslösen einer Warnung

# User Story ID	User Story	Akzeptanzkriterien
E06.01	Als Person, die die App nutzt, möchte ich einen vom medizinischen Fachpersonal oder Test-Center ausgehändigten QR-Code scannen können, damit mir später das Testergebnis in der Corona-Warn-App zur Verfügung gestellt werden kann.	<ol style="list-style-type: none">1. Ein auf dem Flyer des medizinischen Fachpersonals oder Test-Centers vorhandener QR-Code kann mit der Warn-App gescannt werden.2. Erklärungstext wird angezeigt.
E06.02	Als Person, die die App nutzt, möchte ich innerhalb der Corona-Warn-App informiert werden, sobald ein Testergebnis verfügbar ist.	<ol style="list-style-type: none">1. Eine Benachrichtigung informiert lediglich über Neuigkeiten in der App. Das Testergebnis selbst kann nur in der App eingesehen werden.2. Die Benachrichtigung enthält explizit nicht das Ergebnis positiv oder negativ.
E06.03	Bei der Nutzung der App möchte ich, dass bei Vorliegen meines positiven Testergebnisses nach meiner Zustimmung die pseudonymisierten IDs, auf deren Basis ich an den vergangenen Tagen für andere Personen sichtbar war, an den Warn-Server übermittelt werden, damit Kontaktpersonen durch Ihre Apps gewarnt werden können.	<ol style="list-style-type: none">1. IDs können pseudonymisiert an den Warn-Server übermittelt werden.2. Die Übermittlung ist nur möglich, sofern zuvor eine Verifikation erfolgreich durchgeführt wurde. Der Verifikationsserver und die Hotline zum Telefon-TAN Verfahren stellen dies sicher.3. Die Übermittlung ist nur möglich, sofern die Person vorher zugestimmt hat.

**# User
Story
ID**

User Story

Akzeptanzkriterien

E06.04

Bei der Nutzung der App möchte ich neben dem digitalen auch einen manuellen Prozess, z.B. über ein Call-Center nutzen können, damit auch ohne einen vorhandenen QR-Code die pseudonymisierten IDs, unter denen ich in den vergangenen Tagen für andere Personen sichtbar war, an den Warn-Server übermittelt werden, so dass Kontaktpersonen durch Ihre Apps gewarnt werden können.

1. Die zuständige Stelle kann eine TAN generieren und diese der Person mitteilen. (Generiert wird die TAN von einem Server, nicht durch das Call-Center selbst.)

E06.05

Als Person, die die App nutzt, möchte ich die Möglichkeit zur Eingabe einer TAN innerhalb der App haben, damit ich die mir telefonisch mitgeteilte TAN zur Zuordnung meines Testergebnisses zu der von mir genutzten Instanz der App nutzen kann.

1. Die Eingabe einer TAN innerhalb der App ist möglich.

2. Es wird überprüft und zurückgemeldet, ob die eingegebene TAN korrekt war (zu prüfen, ob technisch möglich).

E06.06

Bei der Nutzung der App möchte ich, dass ich nach der Verifikation der TAN meine pseudonymen IDs freiwillig teilen und etwaige Kontaktpersonen warnen kann.

1. IDs können pseudonymisiert an den Warn-Server übermittelt werden.

2. Die Übermittlung ist nur möglich, sofern zuvor eine Verifikation erfolgreich durchgeführt wurde. Der Verifikationsserver und die Hotline zum Telefon-TAN Verfahren stellen dies sicher.

3. Die Übermittlung ist nur möglich, sofern die Person vorher zugestimmt hat.

3.4.7 Parametrisierung

User
Story
ID

User Story

Akzeptanzkriterien

E07.01

Als RKI möchte ich die Parameter zur Risiko-Score-Bestimmung (im Rahmen der technischen Möglichkeiten durch die API) einstellen können, um stets den aktuellen Forschungsergebnissen zur Virusübertragung Rechnung zu tragen.

1. In Abhängigkeit von der bereitgestellten API können Schwellenwerte konfiguriert werden.

2. Die App bezieht dynamische Konfigurationen des RKI, die die Berechnung der Risiko-Einstufung beeinflussen können.

3.4.8 Technische Unterstützung

# User Story ID	User Story	Akzeptanzkriterien
E08.01	Als Person, die die App nutzt, möchte ich eine Hotline kontaktieren können, um technische Probleme mit der App zu lösen	1. Die Telefonnummer der technischen Hotline ist in der App hinterlegt.

3.4.9 Barrierefreiheit

# User Story ID	User Story	Akzeptanzkriterien
E09.01	Als Person, die die App nutzt, möchte ich eine Sprachausgabe nutzen können, um die App (z.B. bei fehlendem oder eingeschränktem Sehvermögen) nutzen zu können.	1. Die Barrierefreiheit bzgl. Sprachausgabe wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.
E09.02	Als Person, die die App nutzt, möchte ich gute Kontraste, veränderbare Schriftgrößen und eine gut lesbare Schriftart haben, um die Texte der App gut lesen zu können.	1. Die Barrierefreiheit bzgl. Kontraste und Schrift wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.
E09.03	Als Person, die die App nutzt, möchte ich, dass mir die Inhalte in einfacher Sprache zur Verfügung gestellt werden, damit ich leicht verstehe, wie ich die App nutzen kann und warum ich es tun sollte.	1. Die Texte und Sprachen werden vom Auftraggeber definiert.

3.4.10 Content Management

# User Story ID	User Story	Akzeptanzkriterien
E10.01	Als RKI möchte ich die Inhalte der App zentral verwalten, um Aktualisierungen von Texten, Links, Hotlines etc. einmalig für alle Stellen in der App durchführen zu können.	<ol style="list-style-type: none">1. Das Content-Management erfolgt auf Grundlage der Anforderungen des RKI2. Der Content wird auf statische und dynamische Inhalte entsprechend der technischen Machbarkeit differenziert3. Aktualisierungen erfolgen in der ersten Version über ein App-Update.

4 Architektur

Gemäß der unter <https://github.com/corona-warn-app/cwa-documentation> veröffentlichten Dokumentation in der bis zur Abnahme / Go-Live-Freigabe nach Abstimmungsvereinbarung jeweils aktuellen Fassung. Bei Widersprüchen zwischen verschiedenen Sprachversionen desselben Dokuments geht die englischsprachige Fassung vor.

www.sap.com/contactsap

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
No part of this publication may be reproduced or transmitted in any form or by any means without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products mentioned by SAP SE and its distributors contain proprietary software components of other software vendors. Mutual product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and technology are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. See www.sap.com/branding for additional trademark information and notices.

THE BEST RUN



ANLAGE 2
FEHLERBEHEBUNGSPROZESSE FÜR CWA-BACKEND- UND FRONTEND-TEIL



Corona-Warn-App

Supportkonzept
Nr. 2020-05-06

PPMS-Objektnummer des Produkts:

CORONA WARN APP SERVER 1.0,
MOB CORONA-WARN 1.0
MOB CORONA-WARN IOS 1.0

Geplanter RTC: Mitte Juni

Solution Owner: XXXXXXXXXX

Genehmigt: 05.06.2020

Dokument-Historie

Version	Datum	Inhalt / Änderung
V0.1	19.05.2020	Erste Version
V0.2	20.05.2020	Entwurf
V0.3	28.05.2020	Interner Review
V0.4	02.06.2020	Änderungen nach Review mit T-Systems hinzugefügt
V0.5	03.06.2020	Datenschutz in Kapitel Störungsbearbeitung hinzugefügt
V0.6	04.06.2020	Änderungen nach Review mit RKI hinzugefügt
V0.7	05.06.2020	Änderungen nach Review mit RKI und T-Systems hinzugefügt
V0.8	05.06.2020	Interner Review
V1.0	05.06.2020	Final

MITWIRKENDE

Organisation	Name	Rolle
SAP Innovative Business Solutions	██████████	Chief Architect
SAP Innovative Business Solutions	██████████	Development Architect
T-Systems	██████████	Head of Cloud Application Operation
T-Systems	██████████	Project Manager

INHALTSVERZEICHNIS

KURZZUSAMMENFASSUNG	5
1. VORWORT	6
2. BESCHREIBUNG DER LÖSUNG UND DES GESCHÄFTSMODELLS	6
2.1 Lösungsüberblick	6
2.2 Wertversprechen für Kunden	7
2.2.1 Übergreifendes Wertversprechen	7
2.2.2 Wertversprechen (Beitrag) vom Support	7
2.3 Anwendungsfälle, Technologie und Architektur	8
2.4 Runbook / Survival Guide	8
3. Supportmodell für die Corona-Warn-App	9
3.1 Übersicht	9
3.1.1 Supportrollen für SAP-bezogene Probleme (Endanwender)	10
3.1.2 Supportrollen für T-Systems-bezogene Probleme (Betriebsstörung)	10
3.2 Supportprozess	12
3.2.1 Rollen	12
3.2.2 Supportprozess nach Rollen	13
3.2.3 Entwicklung, Validierung und Bereitstellung von Code	14
3.2.4 Störungsbearbeitung	20
3.3 Change Management	22
3.3.1 Durch Kunde initiiertes Änderungsantrag	23
3.3.2 Feature Request von Open-Source-Community	23
3.4 Detaillierte Beschreibung des Supportumfangs	24
3.4.1 Mission Critical Support (Support für geschäftskritische Prozesse)	24
3.4.2 Informationsmaterial	26
3.4.3 Zusammenarbeit	27
3.5 Punkte, die nicht im Umfang dieses Supportkonzepts enthalten sind	28
3.5.1 SAP	28
3.6 Supportbedingungen	28
3.7 Fact Sheet	29

ABBILDUNGSVERZEICHNIS

Bildunterschrift 1: Wertversprechen.....	7
Bildunterschrift 2: Supportprozess nach Rollen	13
Bildunterschrift 3: Jenkins-Pipeline.....	14
Bildunterschrift 4: Backend-Bereitstellung	16
Bildunterschrift 5: Sequenzdiagramm für Backend-Bereitstellung	17
Bildunterschrift 6: Frontend-Bereitstellung	17
Bildunterschrift 7: Sequenzdiagramm für Backend-Bereitstellung	18
Bildunterschrift 8: Monitoring-Übersicht.....	19
Bildunterschrift 9: Störung durch Endanwender gemeldet.....	21
Bildunterschrift 10: Störung durch SAP gemeldet	21
Bildunterschrift 11: Änderungsantrag durch Kunde.....	23
Bildunterschrift 12: Feature Request von Community	23

KURZZUSAMMENFASSUNG

Die Corona-Warn-App ist eine neue Cloudlösung, die entwickelt wurde, um die Ausbreitung des Coronavirus einzudämmen.

Es muss ein geeignetes Supportmodell festgelegt werden, um eine reibungslose Betriebsphase der Frontend- und Backend-Entwicklungen der SAP sicherzustellen, die T-Systems für den Betrieb bereitgestellt werden. Die Corona-Warn-App (CWA) ist eine Kooperation zwischen T-Systems, dem Robert Koch-Institut (RKI) und dem Bundesgesundheitsministerium.

In der ersten Phase der Markteinführung wird der SAP-Support für die CWA von den Teams des SAP Solution Management und der Entwicklung geleistet. Das CWA-Team wird:

- sich um die Störungsbearbeitung (eingehende Probleme) kümmern und Probleme nach Bedarf intern an die „zuständigen“ Fachexperten weiterleiten.
- seinen Verpflichtungen hinsichtlich Informationsmaterial, Zusammenarbeit sowie Innovation und Wertschöpfung in einem direkten, personalisierten Austausch mit T-Systems nachkommen.
- die eingehenden Anfragen von der Open-Source-Community über unser Open GitHub mit den zuständigen SAP Community Managern steuern.

T-Systems wird den Mission Critical Support (Support für geschäftskritische Prozesse) für L1/L2 auf Grundlage eines Survival Guide abdecken, der vom SAP CWA Team bereitgestellt wird. Der L3-Support wird direkt vom SAP CWA Team abgedeckt, außer der eigenen Services von T-Systems, die noch im Verantwortungsbereich von T-Systems liegen.

Diese anfängliche Markteinführungsphase soll auch helfen, die Inhalte weiterzuentwickeln, die vom SAP Support für die CWA benötigt werden.

1. VORWORT

Dieses Dokument beschreibt das Supportmodell für die Corona-Warn-App in der ersten Phase der Markteinführung. In dieser Phase soll Feedback vom Markt gesammelt werden, um damit ein stabiles Angebot zu gestalten. Eine strategische Richtung und ein Ausblick für das Supportmodell nach der allgemeinen Verfügbarkeit (Markteinführungsphase) erfordern Validierung, erneute Bestätigung und eine endgültige Entscheidung mit allen Beteiligten.

2. BESCHREIBUNG DER LÖSUNG UND DES GESCHÄFTSMODELLS

2.1 Lösungsüberblick

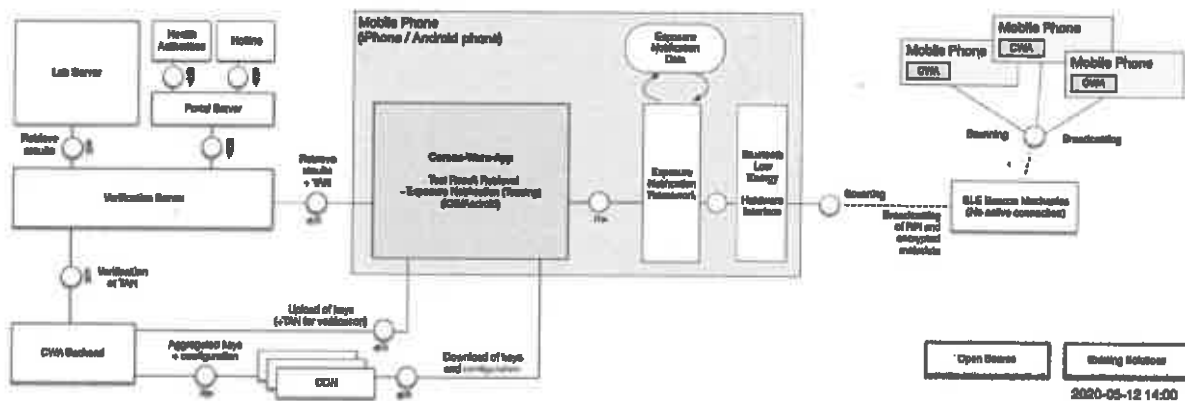


Abbildung 1 Visualisierung der Corona-Warn-App

Mit der Corona-Warn-App¹ können Personen ihr persönliches Kontaktisiko mithilfe ihres Smartphones nachverfolgen. Die hierbei entwickelte Anwendung wird eine neue von Apple und Google zur Verfügung gestellte API, das sogenannte Exposure Notification Framework², nutzen. Beide verwenden die Technologie Bluetooth Low Energy (BLE). Dabei fungieren die einzelnen Smartphones als Beacons (die ständig einen temporären Schlüssel aussenden, an dem sie wiedererkannt werden), während sie gleichzeitig nach IDs anderer Smartphones suchen. Um den Datenschutz zu gewährleisten und die Verfolgung von Bewegungsmustern der Personen zu verhindern, sind die gesendeten IDs nur temporär und ändern sich ständig. Neue IDs werden von einem Schlüssel abgeleitet, der sich täglich durch ein kryptografisches Verfahren ändert.

Die gesammelten IDs anderer Nutzer werden lokal auf dem Smartphone innerhalb der Blackbox des von Apple und Google zur Verfügung gestellten Frameworks gespeichert. Wenn Nutzer positiv auf Covid-19 getestet wurden, können sie der App eine Verifizierung ihres positiven Tests zur Verfügung stellen und eine Option auswählen, dass ihre Schlüssel geteilt werden. Als Folge werden ihre täglichen IDs (Diagnoseschlüssel) der letzten 14 Tage auf einen Server hochgeladen. Auf diesem Server werden alle IDs der Personen, die positiv getestet wurden, aggregiert. Diese Liste aller IDs wird dann allen Smartphones, auf denen die App installiert ist, als Diagnoseschlüssel zur Verfügung gestellt.

Nach dem Herunterladen der Diagnoseschlüssel und der Erkennungskonfiguration werden die Daten an die API übergeben, die in der Lage ist, zu analysieren, ob eine der vom Smartphone gesammelten IDs mit denen einer infizierten Person übereinstimmt. Zusätzlich können Metadaten, die zusammen mit den IDs (z. B. Sendeleistung) gesendet wurden, nun entschlüsselt und verwendet werden.

1 Veröffentlichtes Scoping-Dokument:

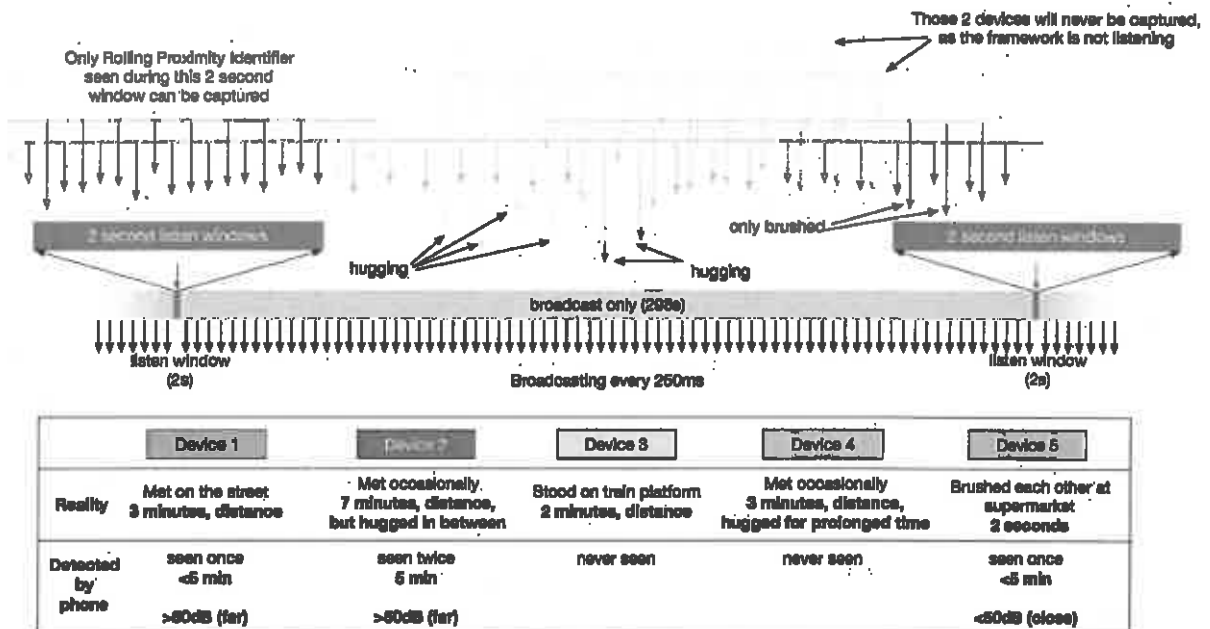
https://github.com/corona-warn-app/cwadocumentation/blob/master/translations/scoping_document.de.md

2 <https://www.apple.com/covid19/contacttracing>

2.2 Wertversprechen für Kunden

2.2.1 Übergreifendes Wertversprechen

Um die Ausbreitung des Coronavirus einzudämmen, ist es mittlerweile notwendig, die Menschen über Kontakte zu anderen Personen zu informieren, die später positiv getestet wurden. Während manche Kontakte, die mit einem persönlichen Gespräch verbunden waren, ermittelt werden können (z.B. Familie, Nachbarn und Kollegen), können viele weitere Kontakte nicht mehr nachvollzogen werden. So kann zum Beispiel in öffentlichen Verkehrsmitteln der Mindestabstand nicht immer eingehalten werden, da hier viele Menschen auf engstem Raum zusammentreffen. Trotzdem kennt die betreffende Person diese Menschen sehr wahrscheinlich nicht.



Bildunterschrift 1: Wertversprechen

2.2.2 Wertversprechen (Beitrag) vom Support

Das SAP-Supportmodell über unser BCP-Meldungssystem ist ein weit verbreitetes Konzept, das eine kontinuierliche und zuverlässige Interaktion im Falle erforderlicher Bugfixes sicherstellt. Die Beteiligten können gemeinsam an den gemeldeten Bugs arbeiten. Die Bearbeitungszeiten werden abhängig von der Priorität sichergestellt, deren Stufen im Abschnitt 3.3.1 Mission Critical Support beschrieben werden.

2.3 Anwendungsfälle, Technologie und Architektur

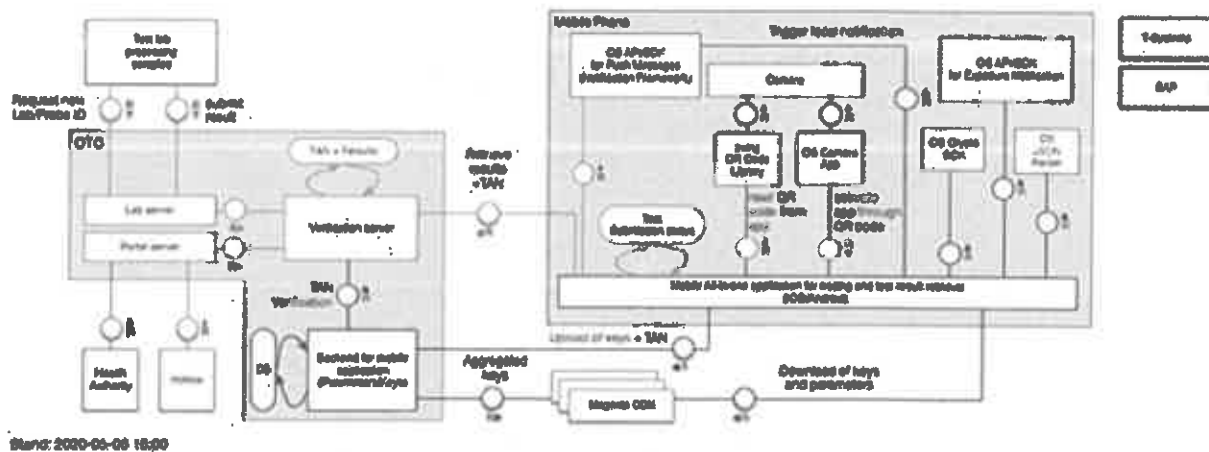


Abbildung 2 Allgemeine Architektur der CWA

Die blauen Komponenten in der Darstellung oben liegen in der Supportverantwortung der SAP. Der Rest liegt in der Verantwortung von T-Systems.

2.4 Runbook / Survival Guide

Die SAP muss für den Betrieb der ausgelieferten Softwarekomponenten ein Runbook/Survival Guide bereitstellen. Dieses Dokument muss alle Konfigurationen, Überwachungs- und Reparaturmaßnahmen beschreiben, die für einen ordnungsgemäßen Betrieb der Software berücksichtigt werden müssen. Im Falle von Problemen, die während der Betriebsphase entdeckt wurden, muss der Guide die Gegenmaßnahmen beschreiben, um die Lösung wieder betriebsbereit zu machen.

3. Supportmodell für die Corona-Warn-App

3.1 Übersicht

Das Supportmodell für die CWA-Lösung ist in drei Level unterteilt. Es wird unterschieden zwischen einer Hotline für Endkundenanfragen und einer Service Line für Störungen im Betriebsablauf. Die folgenden Tabellen zeigen eine Beschreibung der einzelnen Level.

Alle Probleme, die den SAP-eigenen Softwarecode des CWA-Backends und der App auf IOS und Android betreffen, werden von der SAP abgedeckt. Alle Probleme, die den T-Systems-eigenen Softwarecode betreffen, und alle Infrastrukturprobleme, die nicht den Code betreffen, werden von T-Systems abgedeckt.

Die Kommunikation mit den Endanwendern erfolgt über die technische Hotline (Level 1) und löst Probleme beim ersten Anruf mittels einer FAQ Datenbank. Probleme, die nicht gelöst werden können, werden festgehalten und der Clearingstelle (Level 2) weitergeleitet. Dort erfolgt eine Klassifizierung nach Backend oder App Problemen und die entsprechende Weiterleitung an den jeweiligen Level 3 Support.

Der Level-1 der Service Line für Betriebsstörungen läuft rund um die Uhr. Im Prio 1 und 2 Fall wird Level-2-Support im Rahmen der Rufbereitschaft aktiviert. Der Level-3-Support der SAP läuft 8 Stunden an 5 Tagen die Woche während der Geschäftszeiten. Es wird ein „Entwickler in Bereitschaft“-Konzept geben, bei dem ein Entwickler jedes Entwicklungsbereichs nachts und an Wochenenden bei Problemen der Priorität 1 zur Verfügung stehen wird. Die Prioritäten werden in Kapitel 3.3.1 weiter erläutert.

Bei Problemen, die den Code betreffen, und solchen, die nicht den Code betreffen, kann die SAP eine Problemmeldung in SM9 anlegen. (T-Systems Service Desk)

Auf Basis der entsprechenden Priorität und des Schweregrads wird die SAP an einer Lösung für den gemeldeten Bug arbeiten.

Die detaillierten Bugfix-Prozesse für das CWA-Backend und -Frontend werden in 3.2.2 und 3.2.3 beschrieben.

3.1.1 Supportrollen für SAP-bezogene Probleme (Endanwender)

Supportzeiten:



Dies sind die Rollen bei einer Meldung eines Endanwenders:

Level 1 (Telekom)	Level 2 (T-Systems / PU DS)	Level 3 (SAP/ T-Systems PU DS)
Kommunikation mit Endanwendern/Hotline Störungsbearbeitung Sammeln unlösbare Probleme und leiten diese an Level 2 weiter	Klassifiziert die ungelösten Probleme nach Ursache und leitet diese an den jeweiligen Level 3 weiter	Bugfixes Optimierung von Code Stabilisierungsmaßnahmen Migrationen Codeänderungen/Refactoring Verbesserungen von Funktionen Zulieferung von Workarounds für Root Cause Analyses und FAQs

3.1.2 Supportrollen für T-Systems-bezogene Probleme (Betriebsstörung)

Dies sind die Rollen bei einer Meldung, die von der SAP für den T-Systems Service Desk angelegt wird:

Level 1 (T-Systems)	Level 2 (T-Systems / PU PC)	Level 3 (T-Systems / SAP)
Abfangen und Weiterleiten (Meldungen + Änderungen) Service Desk für externe Mitarbeiter und Partner in DE+EN Anlegen von Problemmeldung	Proaktive Anwendungsüberwachung und Benachrichtigungen Störungsbearbeitung Ursachenanalyse Bereitstellung von Workarounds Umsetzung von Reparaturmaßnahmen Verwaltung/Betrieb der Infrastruktur Weiterleitung an Infrastruktur	Bugfixes Optimierung von Code Stabilisierungsmaßnahmen Migrationen Codeänderungen/Refactoring Verbesserungen von Funktionen

Das Supportmodell basiert auf den folgenden Annahmen:

Thema	Bereich	Folge für den Support
Integration	Integration in Validierungsserver und Magenta CDN	Keine durchgängige Supportfähigkeit erforderlich, Weiterleitung von BCP-Meldung gilt als ausreichend.
Geschäftskritisch	Dies ist eine geschäftskritische Lösung mit Rund-um-die-Uhr-Support von T-Systems	SAP-Support steht 8 Stunden an 5 Tagen für Bugfixes während der Geschäftszeiten zur Verfügung und rund um die Uhr für das „Entwickler in Bereitschaft“-Konzept bezüglich P1-Problemen.
Funktionserweiterungen	Obligatorisch und werden mit Änderungsanträgen implementiert	Einschätzung der Auswirkungen auf die Supportbereitstellung ab neuer Releases
Key-User-Konzept	T-Systems muss einen Key User bereitstellen, der für die SAP zur Besprechung einer laufenden Störung erreichbar ist.	Es gelten Standard-Supportprozesse
Infrastruktur	Die Supportbereitstellung im Supportumfang der SAP wird auf der Support-Infrastruktur der SAP basieren (BCP & Support Portal) Probleme bei Infrastruktur oder Backendservices, die im Supportumfang von T-Systems liegen, werden auf der Supportinfrastruktur von T-Systems basieren. (SM9)	Es gelten Standard-Supportprozesse
Supportbereitstellung	T-Systems deckt Geschäftszeiten, Nacht und Wochenende auf Grundlage von Survival Guide und SAP Runbook ab. SAP deckt Meldungen während der Geschäftszeiten und Rufbereitschaft ab.	

3.2 Supportprozess

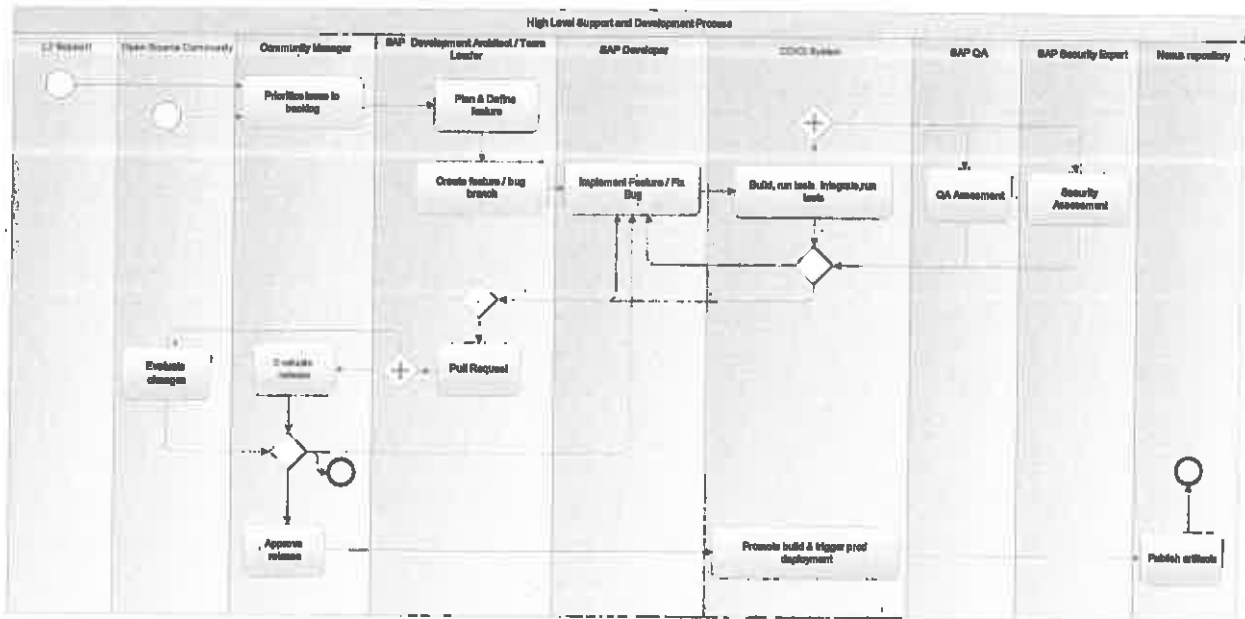
In diesem Abschnitt wird der Gesamtansatz für die Entwicklung neuer Funktionen und Bugfixes für die Anwendung beschrieben. Er berücksichtigt sowohl das angepasste SAP-Arbeitsmodell sowie die hohe Beteiligung der Open-Source-Community.

3.2.1 Rollen

Die an diesem Prozess beteiligten Rollen sind in der folgenden Tabelle beschrieben.

Rolle	Beschreibung
Community Manager	Die Person, die bei der SAP für die Verwaltung der Open-Source-Community für einen bestimmten Funktionsbereich, ein Modul oder eine Anwendung verantwortlich ist
SAP Development Architect / Team Lead	Der SAP-Verantwortliche/Architekt eines bestimmten Moduls, einer Anwendung oder eines Micro-Services, der als Teil dieser Plattform entwickelt wird
SAP Developer	Mitglied des internen Entwicklungsteams mit spezifischen Technologiekenntnissen
SAP UX Designer	Der für die User Experience (Benutzererlebnis) zuständige Designer
SAP QA	Qualitätssicherungsexperte (QA = Quality Assurance)
SAP Security Expert	Der Experte, der für die Sicherheitsaspekte der Plattform verantwortlich ist
SAP DevOps	DevOps-Spezialist, der für die Entwicklungswerkzeuge und den IT-Betrieb verantwortlich ist
Community Manager	Person aus der Open-Source-Community, die den Code im Repository prüft
Open-Source-Community	Person aus der Open-Source-Community, die mit Code zum Repository beiträgt
L2-Support	Level-2-Supportmitarbeiter, der den Bugfixing-Prozess starten kann (empfängt und erfasst Probleme, lädt diese im internen Problemmanagement-System hoch).

3.2.2 Supportprozess nach Rollen



Bildunterschrift 2: Supportprozess nach Rollen

Die Annahme ist, dass Softwareprobleme entweder vom L2-Support oder von der Open-Source-Community erfasst werden. Die Liste der Funktionen und Fehler, die als aktueller Backlog dienen, wird vom Community Manager verwaltet. Dieser filtert und priorisiert die Listeneinträge (hierfür zieht er die entsprechenden Teamleiter und Entwicklungsarchitekten hinzu).

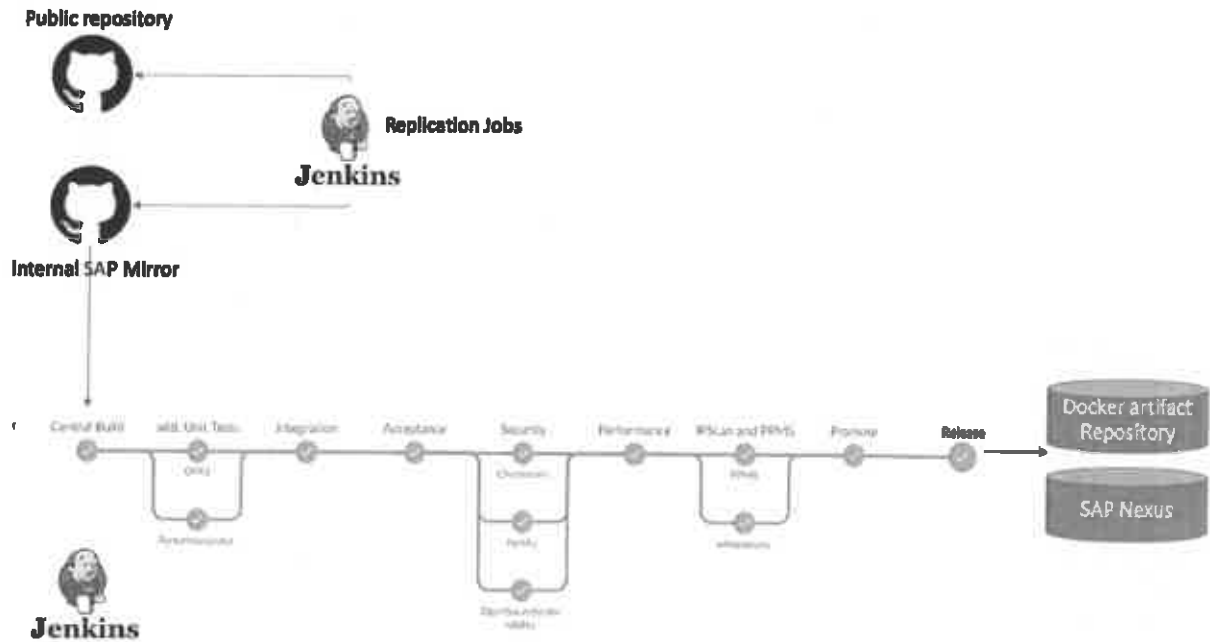
Wird ein Element aus der Liste zur Entwicklung ausgewählt, wird aus dem aktuellen Entwicklungs-Branch ein separater Branch angelegt. Alle weiteren Änderungen werden an diesem speziellen Branch von den Entwicklern vorgenommen.

Für jeden dieser Branches wird eine Continuous Delivery/Continuous Integration Pipeline eingerichtet. Zudem werden Qualitätssicherungs- und Sicherheitsexperten ihre Prüfungen am Code durchführen.

Ist aus Sicht des Entwicklungsteams alles abgeschlossen, wird ein Pull Request an den Entwicklungs-Branch gestellt. Dies wird durch den Community Manager und die Open-Source-Community evaluiert (z. B. zur Ermittlung möglicher Anomalien). Ist alles in Ordnung, wird der Pull Request genehmigt und mit dem Entwicklungs-Branch zusammengeführt. Von hier aus wird eine Package-Pipeline die bereitstellbaren Artefakte in Nexus bauen/publizieren und auf ihren entsprechenden Plattformen bereitstellen (Apple Store, Google Play, Backend-Systeme).

3.2.3 Entwicklung, Validierung und Bereitstellung von Code

CI/CD-Systeme bleiben SAP-intern und entwickeln Module unabhängig auf bestimmten Funktions-/Bug-Banches. Einheiten- und Integrationstests werden als Teil der Pipeline ausgeführt. Statischer Code und Sicherheitsprüfungen werden auch als Teil jedes Builds durchgeführt. Nach erfolgreichem Abschluss des Builds und der Prüfungen werden die Build-Artefakte an die richtigen Repositories gesendet, um für Delivery und Deployment verwendet zu werden. Für jedes Modul werden unabhängige Delivery Pipelines konfiguriert; diese sind mit nur minimalen Abhängigkeiten konzipiert.



Bildunterschrift 3: Jenkins-Pipeline

In dieser Pipeline werden die folgenden Tools und Komponenten genutzt:

Tool	URL
Jenkins (& Grafana)	
Github Internal mirror	
Github Public Repos	
PassVault	
PPMS	
Fortify	
Vulas	
Sonar	
FOSS	
Docker Repository	

3.2.3.1 Code Repository

Das zentrale Code Repository ist das öffentliche GitHub. Die gesamte Codebasis wird über dieses Repository veröffentlicht, geprüft und verwaltet, um Transparenz und Offenheit zu gewährleisten. Über Jenkins-Jobs, die auf der internen SAP-JaaS-Instanz ausgeführt werden, werden die öffentlichen Repositories in das interne SAP GitHub repliziert, wo die Pipelines für Build, Validierung und Deployment gestartet werden.

Richtlinien und Empfehlungen für eine Branch-Strategie zur Verwaltung von Fehlern und Funktionen sowie zu Versions- und Release-Strategien sind im öffentlichen GitHub Repository dokumentiert:

<https://github.com/corona-warn-app/cwa-admin/blob/master/docs/development-organization.md>

Es gibt folgende Arten von Branches:

- Release
- Master
 - Aktueller Entwicklungsstand
- Release-Branches (release/*)
 - zum Fertigstellen eines Major/Minor Release, vom Master abgezweigt
- Hotfix-Branches (hotfix/*)
 - zum Einspielen von Patches in das aktuelle Release
- Feature-Branches (feature/*)
 - zum Fertigstellen eines Major/Minor Release, vom Master abgezweigt

Neue Version (Minor und Major)

1. Abzweigen vom Master mit release/*
2. Update der Version
3. Zusammenführen in Release- und Tag-Version
4. Zusammenführen in Master (neu – SNAPSHOT-Version sollte eingeführt werden)

Hotfixing

1. Abzweigen vom Release mit hotfix/*
2. Fix
3. Update der Patch-Version
4. Wieder in Release zusammenführen

3.2.3.2 Entwicklungsumgebung

Jeder Entwickler hat seine eigene Entwicklungsumgebung. Diese wird pro Workitem-Typ (wie Backend, IOS und Android) individuell an den Workflow und die Bedürfnisse des Entwicklers angepasst. Dennoch sollte jeder Entwickler komplett unabhängig auf seinem Computer entwickeln können und die gesamte benötigte Infrastruktur zur Verfügung haben (z. B. Nutzung eines lokalen Postgres, Dummies/Fakes für Backend-Services, Emulatoren für mobile Endgeräte).

3.2.3.2.1 Backend-Entwicklungsumgebung

Um den Betrieb, die Implementierung und Erweiterung der/des Backend-Server/s für die CWA zu gewährleisten, sollten folgende Tools genutzt bzw. in Betracht gezogen werden:

- Docker
- Kubernetes ist optional und könnte verwendet werden, um dem Entwickler eine Entwicklungs-/Produktivumgebung mit Parität zur Verfügung zu stellen, mit der er lokal arbeiten kann.
- IDE (IE: VS Code, Eclipse, IntelliJ)
- Java JDK
- Terminal zum Ausführen von Shell-Skripten neben verschiedenen installierten Tools wie openssh zum Generieren von selbstsignierten Zertifikaten, kubectf für den Zugriff auf Kubernetes-Cluster sowie alle erforderlichen zusätzlichen Tools, die der Entwickler für geeignet hält.

3.2.3.2.2. Frontend-Entwicklungsumgebung

Um den Betrieb, die Implementierung und Erweiterung der iOS-Version für die CWA zu gewährleisten, sollten folgende Tools genutzt bzw. in Betracht gezogen werden:

- Swift
- IDE (IE: Open Xcode 11.5 Beta 2)
- Lokale Tests (SwiftLint)

Um den Betrieb, die Implementierung und Erweiterung der Android-Version für die CWA zu gewährleisten, sollten folgende Tools genutzt bzw. in Betracht gezogen werden:

- Docker
- Gradle
- Kotlin
- IDE

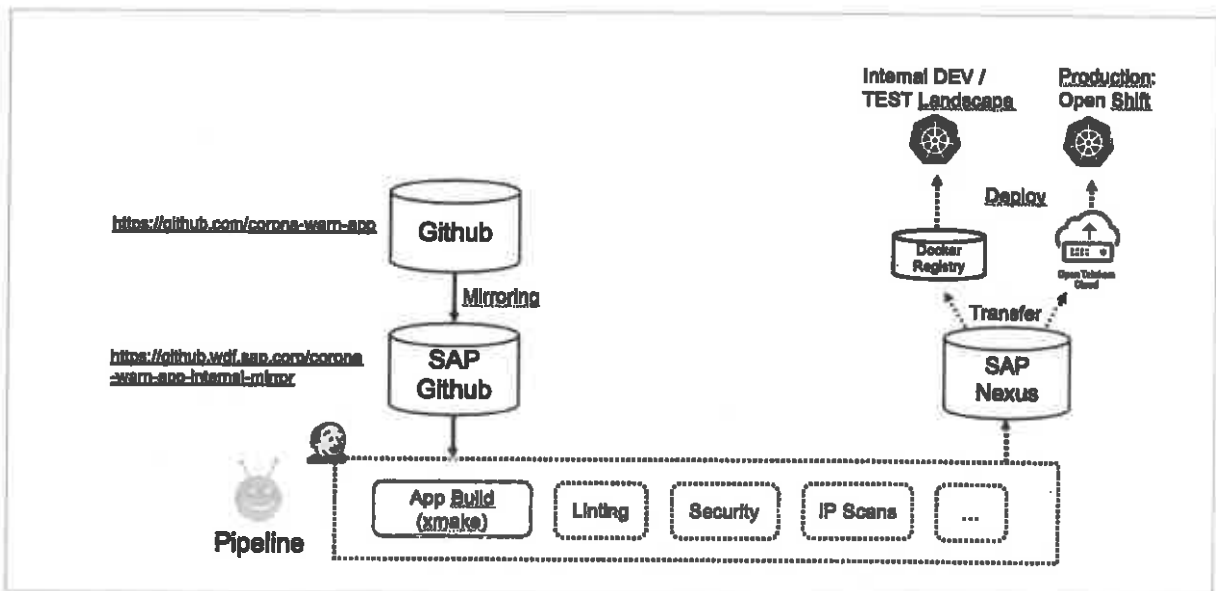
3.2.3.3 **Bereitstellungslandschaft**

Die CWA wird vom Entwicklungsteam nach dem DevOps-Prinzip aufgebaut und betrieben. Eine Pipeline für die Entwicklung und Bereitstellung besteht und wurde von SAP erstellt. Sie läuft auf einem Jenkins CI-Server auf OTC. Die Ausführung wird ausgelöst durch Quellcodeänderungen im öffentlichen GitHub. Implementierungen in Produktivumgebungen werden immer durch manuelle Aktionen ausgelöst. Außerdem gibt es eine zweite Deployment-Landschaft für Entwicklungs-, Qualitätssicherungs- und Testzwecke, die auf der gleichen Infrastruktur basiert.

Folgende Landschaften stehen zur Verfügung:

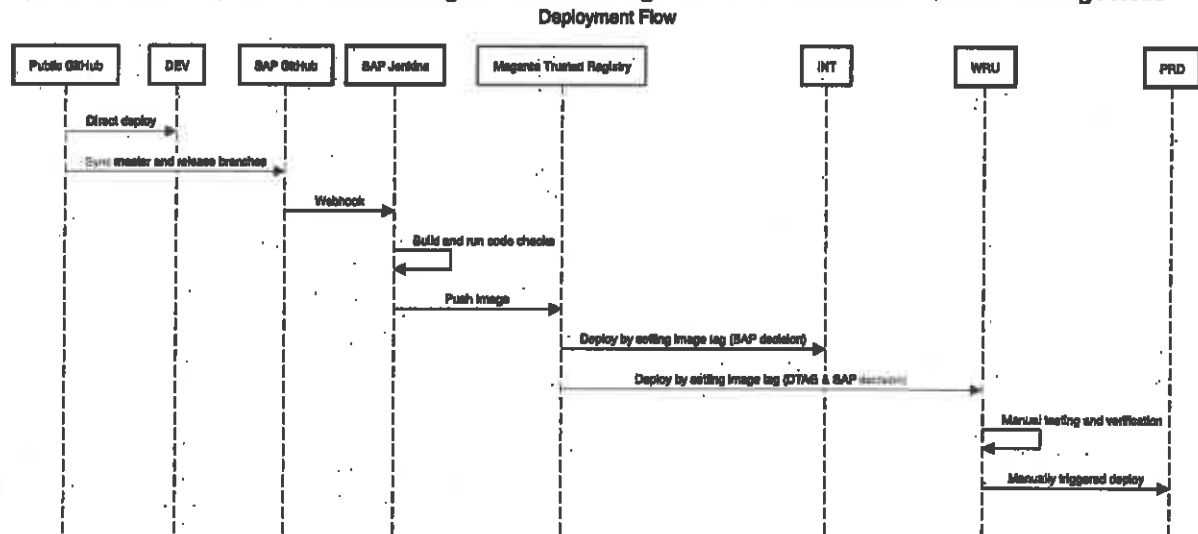
Landschaft	Version
DEV	Master Branch
INT	Aktuelles Minor Release
WRU	Stabiles Minor Release aus Registry
PRD	Manuell genehmigter WRU-Status

3.2.3.3.1 Backend-Bereitstellung



Bildunterschrift 4: Backend-Bereitstellung

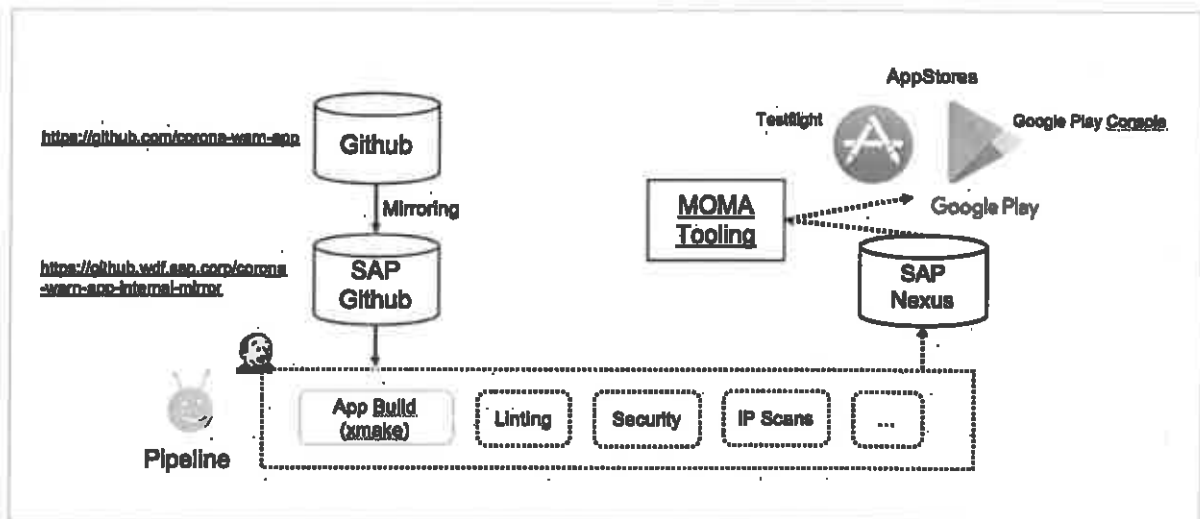
Es gibt eine produktive Bereitstellungsumgebung auf OTC, die von T-Systems für das Hosting der CWA bereitgestellt wird. Das Rechenzentrum befindet sich in Deutschland. Nachdem der Build-Prozess den SAP Nexus erreicht hat, wird die Anwendung als Docker-Image auf einer Kubernetes-Instanz bereitgestellt.



Bildunterschrift 5: Sequenzdiagramm für Backend-Bereitstellung

3.2.3.3.2 Frontend-Bereitstellung

CI / CD Overview: Frontend



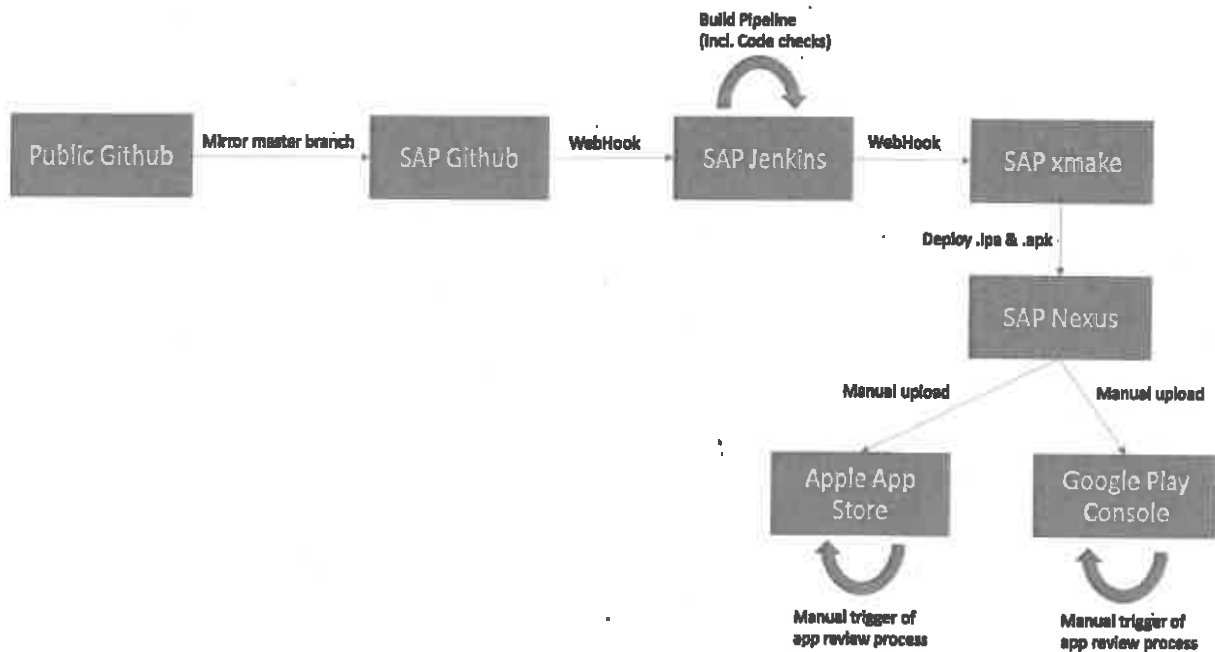
Bildunterschrift 6: Frontend-Bereitstellung

Die Builds werden mit allen erforderlichen Zertifikaten und Bereitstellungsprofilen erstellt. Für die Android-App wird das Zertifikat mit dem Namen „Robert-Koch-Institut“ verwendet, und für die iOS-Version wird das erforderliche Bereitstellungsprofil mit dem RKI-Account angelegt.

Wie oben zu sehen ist, durchläuft jede Implementierung die erforderlichen Sicherheits- und Qualitätsprüfungen. Wenn diese Prüfungen erfolgreich abgeschlossen sind und die Implementierung bereit für den Testeinsatz ist, wird die Testphase gestartet und die Apps werden für Apple Testflight und Google Play Console bereitgestellt. Daher werden von Jenkins Versionen für iOS (.ipa) und Android (.apk) erstellt.

Für das erste Release entwickeln SAP und RKI gemeinsam die Apps für den Apple App Store und den Google Play Store. Alle erforderlichen Metadaten werden von RKI und SAP über MOMA-Tools bereitgestellt. Später werden die Builds jedem der offiziellen Stores bereitgestellt. Die Bereitstellung erfolgt, nachdem ein

Release akzeptiert und der App-Store-Eintrag aktualisiert wurde. Die endgültige Genehmigung neuer Versionen muss in Abstimmung mit dem RKI erfolgen.



Bildunterschrift 7: Sequenzdiagramm für Backend-Bereitstellung

3.2.3.4 Semantische Versionierung

Versionierungsformat: MAJOR.MINOR.PATCH

- MAJOR-Version: Höchstwahrscheinlich nur aufgrund eines neuen Vertrags mit RKI/Deutsche Bundesregierung. Die Kompatibilität mit anderen Major-Versionen ist nicht garantiert.
- MINOR-Version: Neue oder aktualisierte Funktionen. Die Kompatibilität mit anderen Minor-Versionen ist nicht garantiert.
- PATCH-Version: Die Versionsnummer wird mit jedem Hotfix/Patch hochgezählt. Die Kompatibilität mit allen anderen Patch-Versionen innerhalb derselben Minor-Version muss gewährleistet sein. (post 1.0)

3.2.3.5 Integrationsumgebung

Es wird eine SAP-interne Integrationsumgebung zur Verfügung gestellt. Spezifische Integrationstests werden entwickelt, einschließlich aller Module, Anwendungen und Microservices, die am Prozess beteiligt sind. Diese Tests werden durch CI/CD-Systeme gesteuert.

3.2.3.6 Qualitätssicherungs-umgebung

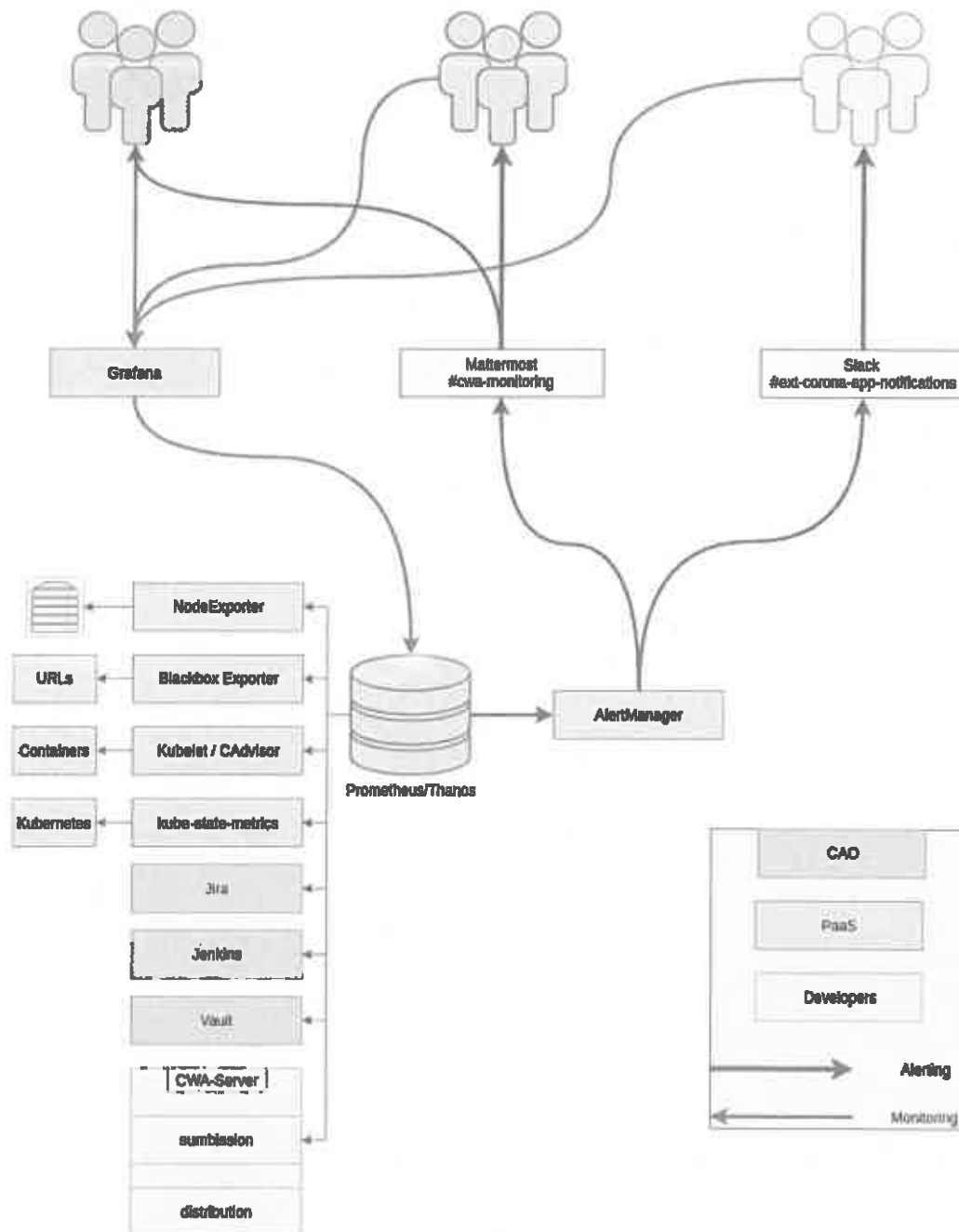
Eine Qualitätssicherungslandschaft wird intern zur Verfügung stehen. Sie wird das aktuelle Image des gesamten Systems haben, damit Tester alle Funktionen manuell testen können.

3.2.3.7 Performance-Testumgebung

Eine Performance-Testing-Landschaft wird intern zur Verfügung stehen. Sie wird so bemessen sein, dass relevante automatisierte Leistungstests periodisch durchgeführt werden können. Diese Umgebung könnte nicht immer, aber auf Anforderungsbasis, bereitgestellt werden.

3.2.3.8 Überwachung

Monitoring und Health Checks werden von T-Systems auf OTC bereitgestellt. In die Cluster wurden auch Prometheus und Grafana installiert, um Metriken zu überwachen und Alerts an einen Slack Channel zu generieren, auf den die Entwicklungs- und Operations-Teams Zugriff haben.



Bildunterschrift 8: Monitoring-Übersicht

3.2.3.9 Abhängigkeiten

Die Anwendungen, die in den Bereich des IBSO-Supports fallen, weisen verschiedene Abhängigkeiten auf, die unten aufgelistet sind. Hier ist es entscheidend, diese Abhängigkeiten und wie sie sich im Laufe der Zeit entwickeln zu verstehen und die bereitgestellten APIs und Protokolle anzupassen.

- Google und Apple API's
- Verification Server
- T-Systems für Infrastruktur

Außerdem finden Sie Ansprechpartner für alle Workstreams, die sich auf die Corona-Warn-App beziehen, im Public GitHub Repository: <https://github.com/corona-warn-app/cwa-admin/blob/master/docs/workstream-contacts.md>

3.2.3.10 Migrationen von APIs

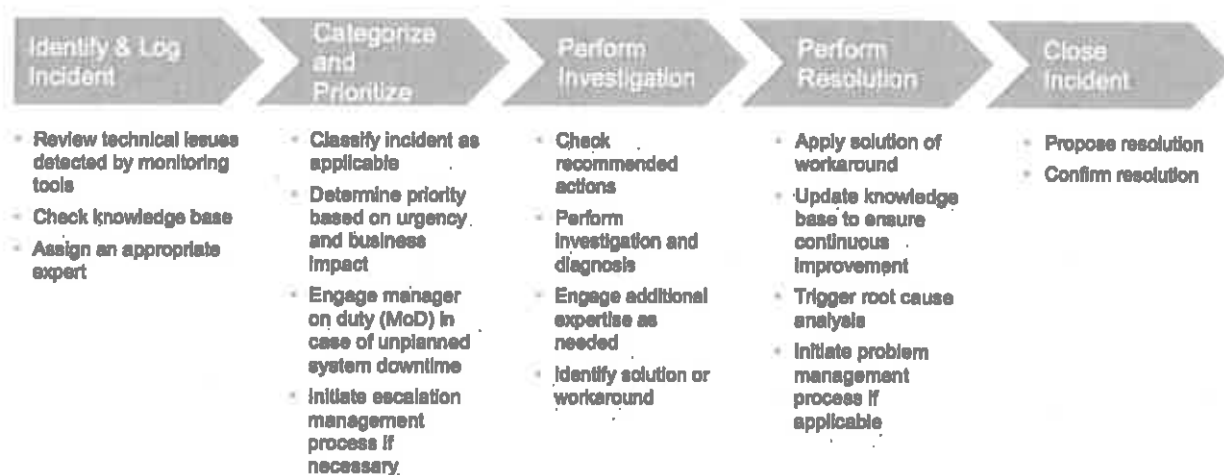
API-Änderungen von Apple und Google, die sich auf die Funktionen der Corona-Warn-App auswirken, müssen in die aktuellste Version migriert werden und sind Teil des Supportprozesses von SAP.

3.2.4 Störungsbearbeitung

In diesem Teil wird der gesamte Prozess der Supportfallbearbeitung beschrieben. Aufgezeigt wird die Zusammenarbeit zwischen Telekom, T-Systems und SAP – vom Anlegen eines Tickets bis zum Bereitstellen einer Lösung.

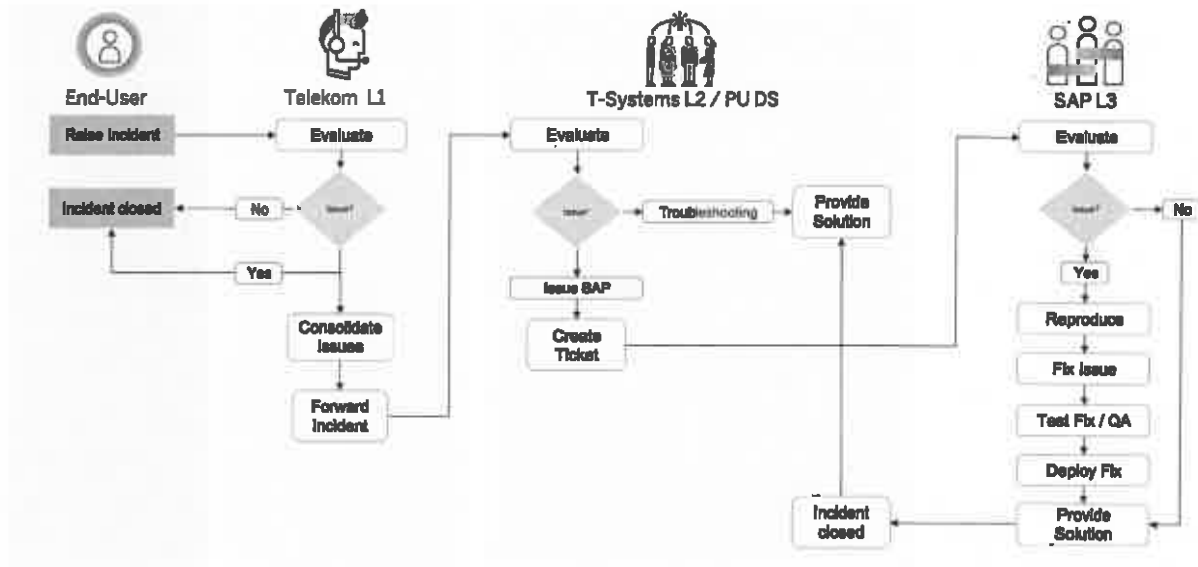
T-Systems trägt dafür Sorge, dass die von T-Systems angelegten Support-Tickets unter den in dieser Anlage genannten Ticketkomponenten eröffnet werden und dass sich in den Support-Tickets außer den Kontaktangaben des Absenders des Support-Tickets keine personenbezogenen Daten befinden. Soweit solche personenbezogenen Daten für den Incident-Management-Prozess entsprechend dieser Anlage erforderlich sind, wird T-Systems diese vor der Übermittlung an SAP schwärzen bzw. anonymisieren.

Nachstehend ein Überblick über den Gesamtprozess der Störungsbearbeitung:



3.2.4.1 Störung durch Endanwender gemeldet

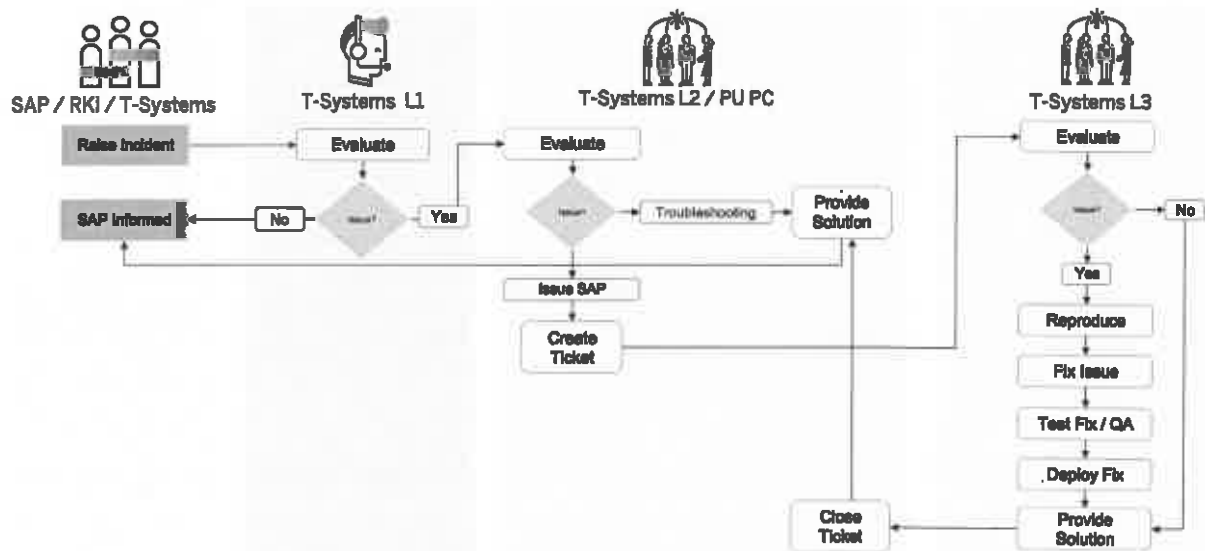
Hier ein Überblick über den Supportprozess aus der Sicht des Endanwenders:



Bildunterschrift 9: Störung durch Endanwender gemeldet

3.2.4.2 Störung durch SAP gemeldet

Hier ein Überblick darüber, wie der Supportprozess aussieht, wenn SAP eine Meldung für T-Systems anlegt:



Bildunterschrift 10: Störung durch SAP gemeldet

3.2.4.1 Priorisierung und Konsolidierung von Problemen

Jeder Vorfall muss entsprechend dem Schweregrad des Problems priorisiert werden, wie in der Service-Level-Vereinbarung in Tabelle 2 angegeben. Es ist auch ersichtlich, dass keine direkte Verbindung zwischen L1- und L2-Support von Telekom zu T-Systems besteht. Alle Meldungen werden zuerst vom L1-Support beantwortet und vom L1-Support geschlossen. Anschließend müssen die Meldungen durch den L1-Support konsolidiert und priorisiert werden, damit sie an den L2-Support und von dort an den SAP-L3-Support weitergeleitet werden können.

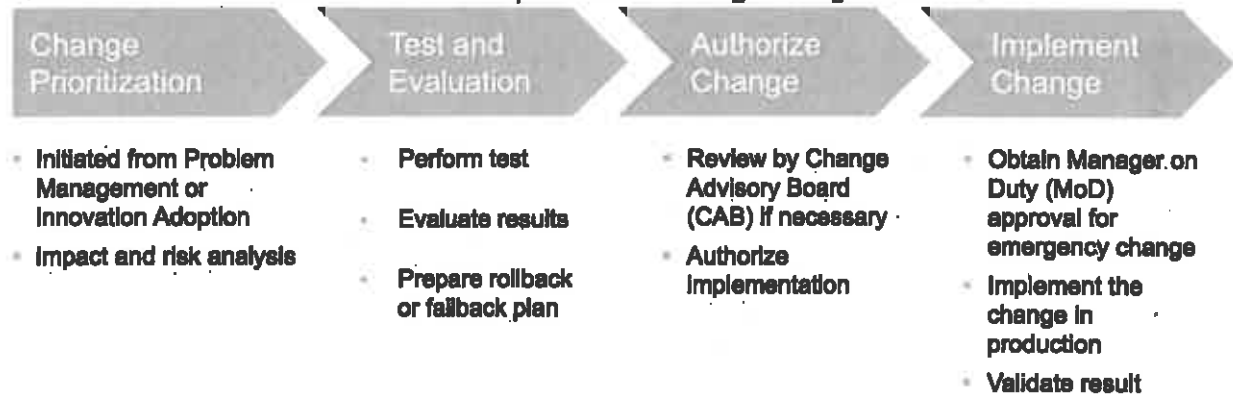
Probleme, die mit P1-P2 gemeldet wurden, müssen mit dem jeweiligen Beteiligten abgestimmt und nach erfolgreichem Abschluss der Quality Gates behoben und die Lösung implementiert werden. Alle Meldungen mit P3-P4 können konsolidiert und die Problemlösungen mit dem nächsten geplanten Bugfix-Release implementiert werden.

3.3 Change Management

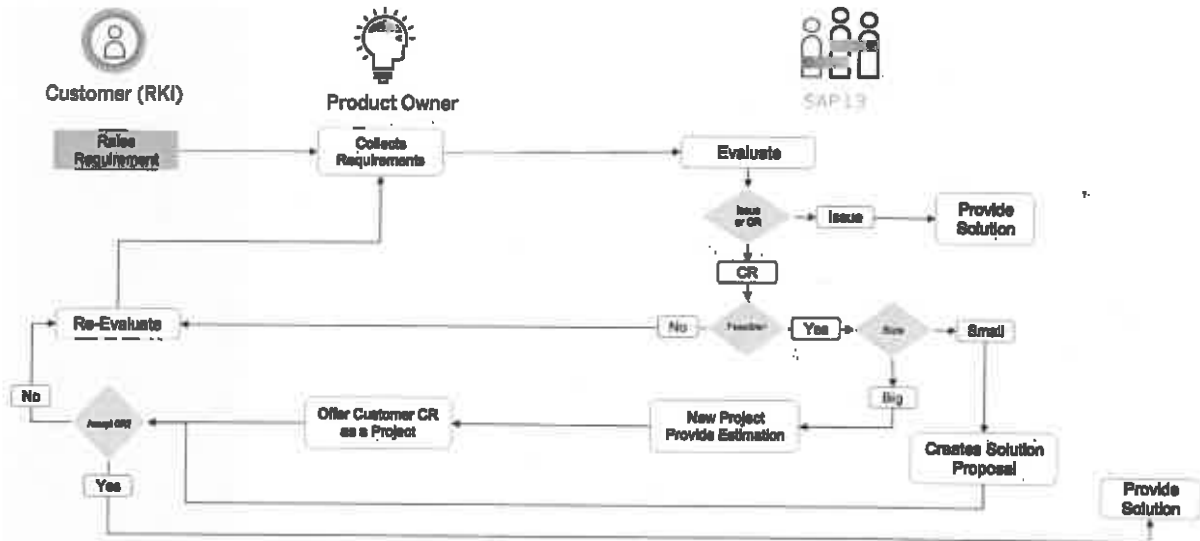
In diesem Teil wird das Change Management im Rahmen des Supportprozesses beschrieben. Aufgezeigt wird die Zusammenarbeit zwischen RKI, Bundesgesundheitsministerium, T-Systems und SAP – vom Anlegen einer Meldung bis zum Bereitstellen einer Lösung.

Das Bundesgesundheitsministerium muss jedem Änderungsantrag, der vom RKI oder der Open-Source-Community angestoßen wurde, zustimmen.

Nachstehend ein Überblick über den Gesamtprozess des Change Managements:

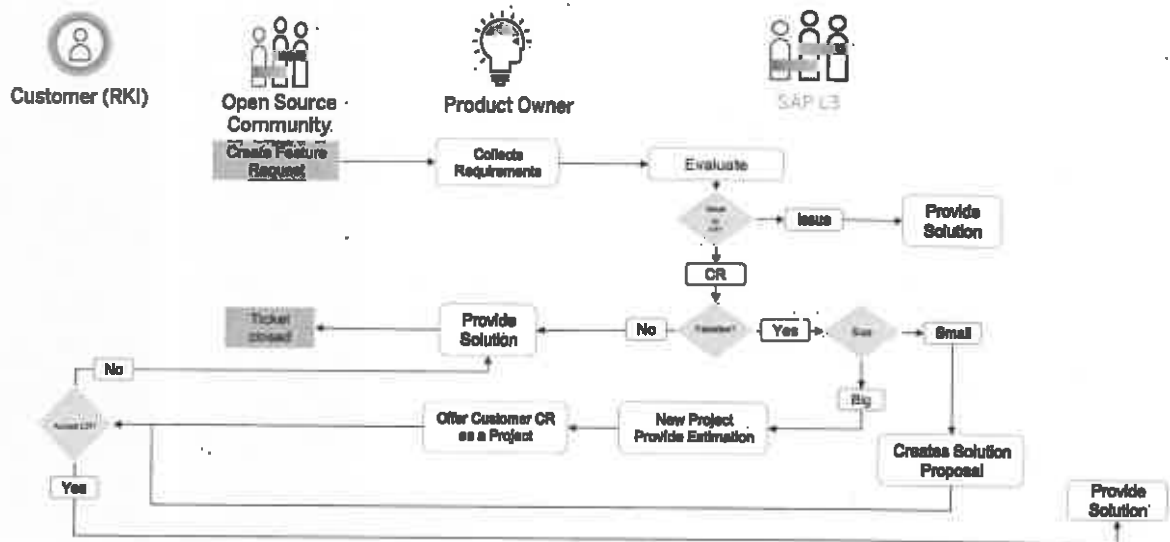


3.3.1 Durch Kunde Initiierter Änderungsantrag



Bildunterschrift 11: Änderungsantrag durch Kunde

3.3.2 Feature Request von Open-Source-Community



Bildunterschrift 12: Feature Request von Community

3.4 Detaillierte Beschreibung des Supportumfangs

3.4.1 Mission Critical Support (Support für geschäftskritische Prozesse)

SAP reagiert auf übermittelte Supportfälle (auch als „Fall“, „Meldung“ oder „Problem“ bezeichnet), wie in der folgenden Tabelle dargelegt. Zusätzlich werden die Supportlevel nach der Priorität abgebildet, die von T-Systems vergeben wird:

Priorität		Definition	Reaktionsstufe
T-Systems	SAP		
P1	P1	<p>Sehr hoch: Eine Meldung ist mit der Priorität „Sehr hoch“ einzustufen, wenn das Problem sehr schwerwiegende Auswirkungen auf normale Geschäfts- oder IT-Prozesse hat, die in Verbindung mit Kerngeschäftsprozessen stehen. Dringende Arbeiten können nicht durchgeführt werden.</p> <p>Dies wird in der Regel durch folgende Umstände verursacht:</p> <ul style="list-style-type: none"> - Ein produktiver Service ist vollständig ausgefallen. - Unmittelbar bevorstehende Produktivstarts oder Upgrades können nicht abgeschlossen werden. - Die Kerngeschäftsprozesse des Kunden sind ernsthaft beeinträchtigt. <p>Eine Behelfslösung (Workaround) ist nicht für jeden Umstand verfügbar. Die Meldung erfordert eine sofortige Bearbeitung, weil es durch die Fehlfunktion zu erheblichen Verlusten kommen kann.</p>	<p>Reaktionszeit: Innerhalb einer Stunde nach Eingang des Supportfalls</p>
P2	P2	<p>Hoch: Eine Meldung ist mit der Priorität „Hoch“ einzustufen, wenn normale Geschäftsprozesse stark beeinträchtigt werden. Notwendige Arbeiten können nicht durchgeführt werden. Die Störung wird verursacht durch fehlerhafte oder nicht ausführbare Funktionen im SAP-Service, die unmittelbar benötigt werden.</p> <p>Die Meldung muss so schnell wie möglich bearbeitet werden, weil es durch die anhaltende Fehlfunktion zu ernsthaften Unterbrechungen des gesamten produktiven Geschäftsablaufs kommen kann.</p>	<p>Reaktionszeit: Innerhalb einer Stunde nach Eingang des Supportfalls</p>
P2	P3	<p>Mittel: Eine Meldung ist mit der Priorität „Mittel“ einzustufen, wenn normale Geschäftsprozesse beeinträchtigt werden. Das Problem wird verursacht durch fehlerhafte oder nicht ausführbare Funktionen im SAP-Service.</p>	<p>Reaktionszeit: Innerhalb eines Geschäftstages nach Eingang des Supportfalls beim SAP-Support</p>
P3	P4	<p>Niedrig: Eine Meldung ist mit der Priorität „Niedrig“ einzustufen, wenn das Problem nur geringe oder keine Auswirkungen auf die normalen Geschäftsprozesse hat. Das Problem wird durch fehlerhafte oder nicht ausführbare Funktionen im SAP-Service verursacht, die nicht täglich oder nur selten benötigt werden.</p>	<p>Reaktionszeit: Innerhalb von zwei Geschäftstagen nach Eingang des Supportfalls beim SAP-Support</p>

Tabelle 1: Service-Level-Vereinbarungen

3.4.1.1 Rund-um-die-Uhr-Support für geschäftskritische Prozesse für P1- und P2-Probleme

Zu erbringende Leistung	Wird erbracht von
Einen „Survival Guide“ für die Überwachung von P1/2 zur Verfügung stellen	<ul style="list-style-type: none"> • SAP / • T-Systems
Supportmitarbeiter schulen und ihnen Know-how vermitteln	<ul style="list-style-type: none"> • SAP / • T-Systems
Reaktionszeit	
Reaktionszeit während der Geschäftszeiten erfüllen	<ul style="list-style-type: none"> • T-Systems
Ein „Sicherheitsnetz“ bereitstellen <ul style="list-style-type: none"> • Support QM überwacht • Supportmitarbeiter erfüllt Reaktionszeit 	<ul style="list-style-type: none"> • T-Systems
Reaktionszeit außerhalb der Geschäftszeiten erfüllen	<ul style="list-style-type: none"> • T-Systems

Info: SAP-interne Vorgehensweise beim Ausfall des Produktivsystems

P1-Probleme werden SAP-intern als „Ausfall des Produktivsystems“ eingestuft, wenn folgende Kriterien erfüllt sind.

Ausfall des Produktivsystems = die zentralen Business Services sind durch folgende Faktoren erheblich beeinträchtigt:

- Der Service ist überhaupt nicht verfügbar oder kann vom Kunden nicht abgerufen werden oder
- Der Service ist fast nicht nutzbar aufgrund einer sehr schlechten Performance, was zu erheblichen Verzögerungen im Geschäftsbetrieb führt oder
- Der Service ist fast nicht nutzbar, da er häufig nicht verfügbar ist, oder der Service liefert falsche Daten oder falsche Ergebnisse.

Die Behandlung von Ausfällen des Produktivsystems hat in erster Linie das Ziel, die Services wieder zum Laufen zu bringen (wofür das eigentliche Problem nicht immer behoben werden muss).

P1-Probleme, die als „Ausfall des Produktivsystems“ eingestuft werden, werden in Zusammenarbeit mit T-Systems und dem Development Support der SAP von den Mission Control Centers nach einem Rund-um-die-Uhr-Konzept behandelt. Für jeden Ausfall eines Produktivsystems wird ein verantwortlicher Deeskalationsarchitekt bestimmt, der den Kommunikations- und Lösungsprozess zwischen allen beteiligten Bereichen innerhalb der SAP, dem Kunden und den beteiligten Partnern steuert.

„Unter Kontrolle“ bedeutet:

- Das Problem ist behoben und produktiv im System, das den Geschäftsservice des Kunden steuert.
- Eine zuverlässige Behelfslösung ist verfügbar, die einen kontinuierlichen Betrieb gewährleistet, bis die endgültige Korrektur implementiert ist.
- Ein Maßnahmenplan für Korrekturen ist vorhanden (z. B. für das Wiederherstellungsverfahren als letzter Plan B).

3.4.1.2 Support für nicht geschäftskritische Prozesse für P3- und P4-Probleme (nur Englisch) während der Geschäftszeiten

Zu erbringende Leistung	Wird erbracht von
Reaktionszeit während der Geschäftszeiten erfüllen	<ul style="list-style-type: none"> • T-Systems
Bei einem funktionalen Problem stellt das SAP-Entwicklerteam einen Bugfix innerhalb eines angemessenen Zeitraums bereit.	<ul style="list-style-type: none"> • SAP

3.4.2 Informationsmaterial

3.4.2.1 Informationen zu Release-Updates

Zu erbringende Leistung	Wird erbracht von
Lösungsspezifischen Content über den App Store zur Verfügung stellen	<ul style="list-style-type: none"> • SAP • RKI
Informationen zu Release-Updates zur Verfügung stellen (Frontend)	<ul style="list-style-type: none"> • SAP • RKI
Informationen zu Release-Updates zur Verfügung stellen (Backend)	<ul style="list-style-type: none"> • SAP • T-Systems

3.4.3 Zusammenarbeit

3.4.3.1 Support über den App Store

Zu erbringende Leistung	Wird erbracht von
Der Community-Manager konzentriert sich auf Probleme, die im App Store angelegt werden, und legt im Falle eines Problems eine Meldung im Supportsystem an.	<ul style="list-style-type: none"> SAP

3.4.3.2 Support per E-Mail

Zu erbringende Leistung
SAP und T-Systems stellen eine interne E-Mail-Verteilerliste zur Verfügung, mit der die Entwickler im Falle eines wichtigen Problems direkt kontaktiert werden können. T-Systems: [REDACTED]

3.4.3.3 Support über die Hotline

Zu erbringende Leistung	Wird erbracht von
Die Telekom stellt eine Hotline für Endanwender zur Verfügung, an die man sich bei Problemen auch wenden kann. Anschließend werden die Meldungen als neue Support-Tickets an den L2-Support der Telekom weitergeleitet. Hotline: [REDACTED]	<ul style="list-style-type: none"> Telekom

3.4.3.4 Support per Chat

Zu erbringende Leistung	Wird erbracht von
Der interne Support per Chat wird von SAP über Slack zwischen SAP- und T-Systems-Entwicklern erbracht. URL: [REDACTED]	<ul style="list-style-type: none"> SAP

3.4.3.5 Support über L2/L3 Support

Zu erbringende Leistung	Wird erbracht von
Bei Problemen wird SAP eine Meldung direkt beim T-Systems Service Desk L1 anlegen und die Kommunikation dort verfolgen.	<ul style="list-style-type: none"> T-Systems
BCP (Support Portal) wird von SAP als zentrales Meldungssystem verwendet werden. Bei Problemen wird T-Systems eine Meldung direkt in BCP anlegen und die Kommunikation dort verfolgen.	<ul style="list-style-type: none"> SAP

3.5 Punkte, die nicht im Umfang dieses Supportkonzepts enthalten sind

Punkte, die für die jeweilige Partei nicht im Umfang des Supportkonzepts enthalten sind:

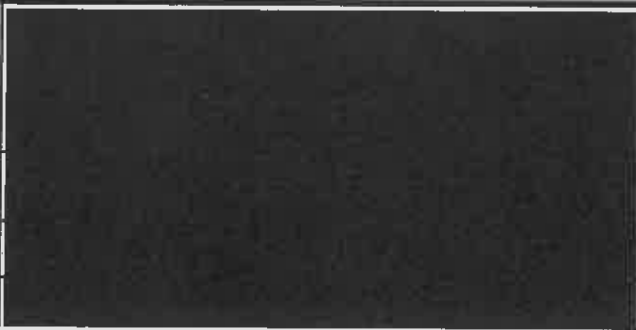
3.5.1 SAP

- Hosting/Betrieb von Backend und Frontend, inklusive Service-Level-Vereinbarungen
- Entwicklung und Betrieb des Verifizierungsservers
- Entwicklung und Betrieb des Portalservers
- Integration der Labore
- Kommunikations-Hotline für Endanwender
- Support für Endnutzer/Verbraucher

3.6 Supportbedingungen

Informationen hierzu finden Sie unter <http://go.sap.com/about/agreements.sap-cloud-services-customers.html>.

3.7 Fact Sheet

Thema	Beschreibung
BCP-Komponente(n)	
Support-Mail-Verteiler	
Slack Channel	
Hotline Telekom	

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.asp#trademark> for additional trademark information and notices. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.
These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.



**ANLAGE 3
GOVERNANCE**

1. ABSTIMMUNGEN UND ENTSCHEIDUNGEN ZWISCHEN AUFTRAGGEBER UND DEN INDUSTRIEPARTNERN

1.1 Zentrales Entscheidungsgremium

1. Die Parteien richten ein zentrales Entscheidungsgremium ein, um die für die Zusammenarbeit relevanten Entscheidungen und Abstimmungen, gemeinsam treffen zu können. Gleichzeitig dient das zentrale Entscheidungsgremium zur Lösung von Meinungsverschiedenheiten zwischen den Parteien (Funktion als vorgeschaltetes Eskalationsgremium).
2. Mitglieder des zentralen Entscheidungsgremiums sind Vertreter des BMG bzw. RKI, von SAP und T-Systems sowie des BKAmts und des BMI.
3. Für alle Entscheidungen des zentralen Entscheidungsgremiums besteht ein grundsätzliches Einstimmigkeitsgebot. Kommt keine Einstimmigkeit zustande, genügt die Zustimmung des BMG als Vertreter des Auftraggebers und desjenigen Industriepartners, dessen Leistungsbereich betroffen ist.
4. Das zentrale Entscheidungsgremium tagt in der Entwicklungsphase und in den ersten 14 Tagen nach GO-Live bis auf Weiteres in der Regel täglich und anschließend wöchentlich (sowie zusätzlich bei Bedarf).
5. Die Industriepartner erstatten dem zentralen Entscheidungsgremium Bericht über den jeweils aktuellen Projektstand sowie wesentliche Vorkommnisse in Bezug auf Entwicklung und Betrieb des Gesamtsystems. Auf Verlangen des Auftraggebers sind die jeweiligen Projektleiter der Industriepartner zu Sitzungen des zentralen Entscheidungsgremiums hinzuziehen, um den Mitgliedern Fragen zu beantworten und Auskünfte zu erteilen.
6. Die Einbringung von Entscheidungs- und Abstimmungsbedarf erfolgt vorab per schriftlicher Übermittlung. Die Vorstellung des Entscheidungs- und Abstimmungsbedarfs erfolgt durch das jeweils einbringende Mitglied.
7. Die Entscheidungen und Festlegungen des zentralen Entscheidungsgremiums werden schriftlich protokolliert. Die Protokollierung erfolgt durch einen der Industriepartner. Das Protokoll wird am jeweils nächsten Werktag an alle Mitglieder versandt. Erfolgen keine Einwände innerhalb von 2 (zwei) Werktagen (während der Entwicklungsphase) bzw. innerhalb von 10 (zehn) Werktagen (nach der Entwicklungsphase) ab Erhalt des Protokolls gilt das Protokoll als von allen Mitgliedern genehmigt.
8. Soweit eine Entscheidung des zentralen Entscheidungsgremiums zu einer Änderung der von einem der Industriepartner vertraglich geschuldeten Leistungen, etwa bezüglich des Leistungsinhalt, Leistungsumfang, Leistungsqualität, Zeitpunkt und Ort sowie Art und Weise der Leistungserbringung oder der rechtlichen Regelungen des Vertrags zwischen Auftraggeber und einem der Industriepartner führt, wird die Entscheidung

des zentralen Entscheidungsgremiums erst verbindlich, wenn eine Änderungsvereinbarung zwischen dem Auftraggeber und dem jeweiligen Industriepartner gemäß des vertraglichen Change Request-Verfahrens abgeschlossen wurde.

9. Soweit sich die Mitglieder nicht auf eine einvernehmliche Entscheidung im gemeinsamen Entscheidungsgremium verständigen können, kann jedes Mitglied den Entscheidungsgegenstand in das zentrale Strategie- und Eskalationsgremium gemäß Ziff. 1.2 einbringen.

1.2 Zentrales Strategie- und Eskalationsgremium

1. Die Parteien richten ein zentrales Strategie- und Eskalationsgremium ein, um übergreifende, strategische Entscheidungen und Abstimmungen treffen zu können und gleichzeitig als Eskalationsgremium bei Meinungsverschiedenheiten zu einer einvernehmlichen Lösung zu gelangen.
2. Mitglieder des zentralen Strategie- und Eskalationsgremiums sind die Bundesminister des BMG sowie Vorstandsmitglieder und Projektleiter der SAP und T-Systems sowie während der Entwicklungsphase die Bundesminister des BKamts und des BMI.
3. Für alle Entscheidungen des zentralen Entscheidungsgremiums besteht ein grundsätzliches Einstimmigkeitsgebot. Kommt keine Einstimmigkeit zustande, genügt die Zustimmung des BMG als Vertreter des Auftraggebers und desjenigen Industriepartners, dessen Leistungsbereich betroffen ist.
4. Das zentrale Strategie- und Eskalationsgremium tagt während der Entwicklungsphase bis auf Weiteres in der Regel wöchentlich und nach GO-Live bei Bedarf.
5. Die Einbringung von Entscheidungs- und Abstimmungsbedarf, einschließlich im Falle von Meinungsverschiedenheiten gemäß Ziff. 1.1 Abs. 8, erfolgt vorab per schriftlicher Übermittlung. Die Vorstellung des Entscheidungs- und Abstimmungsbedarfs erfolgt durch das jeweils einbringende Mitglied.
6. Die Entscheidungen und Festlegungen des zentralen Strategie- und Eskalationsgremiums werden schriftlich protokolliert. Die Protokollierung erfolgt durch einen der Industriepartner. Das Protokoll wird am jeweils nächsten Werktag an alle Mitglieder versandt. Erfolgen keine Einwände innerhalb von 2 (zwei) Werktagen (während der Entwicklungsphase) bzw. innerhalb von 10 (zehn) Werktagen (nach der Entwicklungsphase) ab Erhalt des Protokolls gilt das Protokoll als von allen Mitgliedern genehmigt.
7. Sollten sich die Mitglieder bei Meinungsverschiedenheiten im zentralen Strategie- und Eskalationsgremium nicht innerhalb von maximal 2 (zwei) Wochen auf eine einvernehmliche Lösung verständigen können, bleibt es dem Auftraggeber und jedem der Industriepartner unbenommen, ein [Schiedsverfahren / Gerichtsverfahren] gemäß der jeweiligen Vertragsbedingungen zwischen Auftraggeber und dem jeweiligen bzw. den Industriepartnern einzuleiten.

2. ABSTIMMUNGEN UND ENTSCHEIDUNGEN ZWISCHEN DEN INDUSTRIEPARTNERN UNTEREINANDER

2.1 Projektleitungs-Jour-Fixe

1. Die Projektleiter der Industriepartner werden die für die Zusammenarbeit relevanten Entscheidungen und Abstimmungen in einem gemeinsamen Projektleitungs-Jour-Fixe treffen.
2. Der Projektleitungs-Jour-Fixe findet in der Entwicklungsphase und in den ersten 14 Tagen nach GO-Live bis auf Weiteres in der Regel zweimal täglich (morgens und abends) und anschließend wöchentlich (sowie zusätzlich bei Bedarf) statt.
3. Die Einbringung von Entscheidungs- und Abstimmungsbedarf bedarf keiner zwingenden vorherigen schriftlichen Übermittlung.
4. Soweit sich die Projektleiter der Industriepartner nicht auf eine einvernehmliche Entscheidung im Projektleitungs-Jour-Fixe verständigen können, kann jeder Projektleiter den Entscheidungsgegenstand in Vorstands-Jour-Fixe gemäß Ziff. 2.2 einbringen.

2.2 Vorstands-Jour-Fixe

1. Die Industriepartner werden wichtige Themen, insbesondere bei Meinungsverschiedenheiten gemäß Ziff. 2.1 Abs. 5, in einem gemeinsamen Vorstands-Jour-Fixe treffen.
2. Der Vorstands-Jour-Fixe findet in der Entwicklungsphase bis auf Weiteres in der Regel einmal täglich statt und nach GO-Live bei Bedarf.
3. Die Einbringung von Entscheidungs- und Abstimmungsbedarf, einschließlich im Falle von Meinungsverschiedenheiten gemäß Ziff. 2.1 Abs. 5, erfolgt vorab per schriftlicher Übermittlung. Die Vorstellung des Entscheidungs- und Abstimmungsbedarfs erfolgt durch den jeweils einbringenden Projektleiter.
4. Soweit sich die Industriepartner nicht auf eine einvernehmliche Entscheidung im Vorstands-Jour-Fixe verständigen können, kann jeder Industriepartner den Entscheidungsgegenstand in das zentrale Entscheidungsgremium gemäß Ziff. 1.1 einbringen.

3. SONSTIGE ABSTIMMUNGEN AUF ARBEITSEBENE

3.1 Laufende Abstimmungen auf Arbeitsebene zwischen den Industriepartnern untereinander

1. Die laufende Abstimmung zwischen den Industriepartnern auf Arbeitsebene während der Entwicklungsphase erfolgt innerhalb der Workstreams im Rahmen von in der Regel täglichen Workstream-Updates sowie durch die Workstream-Leads im Rahmen von in der Regel ebenfalls täglichen Scrum Status Updates und nach GO-Live bei Bedarf.

2. Im Falle von sich hieraus ergebenden Entscheidungsbedarfs, insbesondere im Falle des Erkennens von Risiken und Unklarheiten sowie im Falle von Meinungsverschiedenheiten erfolgt eine Eskalation über die Workstream Leads an den Projektleitungs-Jour-Fixe gemäß Ziff. 2.1.
3. Der an den Projektleitungs-Jour-Fixe zu adressierende Entscheidungs- und Mitteilungsbedarf sowie sonstige bedeutsame Festlegungen auf Arbeitsebene im Rahmen der Workstream-Updates und Scrum Status Updates wird schriftlich protokolliert. Die Protokollierung erfolgt nach Absprache durch einen der Industriepartner. Das Protokoll wird noch am selben Werktag an den jeweils anderen Industriepartner versandt. Erfolgen keine Einwände innerhalb von 1 (einem) Werktag ab Erhalt des Protokolls gilt das Protokoll als von beiden Industriepartnern genehmigt.

3.2 Laufende Abstimmungen auf Arbeitsebene der Industriepartner mit weiteren Projektbeteiligten

1. Neben der laufenden Abstimmung zwischen den Industriepartnern untereinander erfolgt eine Abstimmung der Industriepartner mit weiteren Projektbeteiligten auf Arbeitsebene im Rahmen von regelmäßigen Terminen sowie bei Bedarf. In die Abstimmung ist der Auftraggeber jeweils einzubeziehen.
2. Die weiteren Projektbeteiligten sind BSI, BfDI, Fraunhofer sowie Apple und Google.
3. Die Festlegungen bei den Abstimmungen zwischen den Industriepartnern und den weiteren Projektbeteiligten werden schriftlich protokolliert. Die Protokollierung erfolgt nach Absprache durch einen der Industriepartner. Das Protokoll wird am jeweils nächsten Werktag an die Industriepartner, die jeweiligen weiteren Gesprächsteilnehmer und an den Auftraggeber versandt.
4. Im Falle von Entscheidungs- oder Mitteilungsbedarfs, insbesondere im Falle des Erkennens von Risiken und Unklarheiten sowie im Falle von Meinungsverschiedenheiten bei den Abstimmungen zwischen den Industriepartnern, dem Auftraggeber und den weiteren Projektbeteiligten erfolgt eine Eskalation über die Projektleiter der Industriepartner an das zentrale Entscheidungsgremium gemäß Ziff. 1.1.

**ANLAGE 4
DOKUMENTATION**

ANLAGE 4 DOKUMENTATION

Nr.	Dokumentation	Kon- sol- dierun- g	SAP-Teile	TSI-Teile	Termin	Sprache
1.	Gesamtarchitektur: Übersicht aller Komponenten (App und Backend-Komponenten; sonstige beteiligte Komponenten)	SAP	Architektur-Dokument (GitHub): https://github.com/corona-wam-app/cwa-documentation/blob/master/solution_architecture.md		veröffentlicht	Englisch
2.	Funktionalität der Komponenten: Genaue und vollständige Beschreibung der Funktionalität aller Komponenten	SAP/TSI	Scoping Dokument (GitHub): https://github.com/corona-wam-app/cwa-documentation/blob/master/scoping_document.md	Scoping Dokument: https://github.com/corona-wam-app/cwa-documentation/blob/master/scoping_document.md Details zu den Funktionalitäten sind in folgenden Software Design Dokumenten beschrieben: a) Verification Server: https://github.com/corona-wam-app/cwa-verification-server/blob/master/docs/architecture-overview.md b) Test Result Server: https://github.com/corona-wam-app/cwa-testresult-server/blob/master/docs/architecture-overview.md c) Portal Server – Verification Portal: https://github.com/corona-wam-app/cwa-verification-portal/blob/master/docs/architecture-overview.md	veröffentlicht	Englisch
3.	System- und Betriebedokumentation für Komponenten	SAP/TSI	Supportkonzept	Betriebshandbuch gemäß Telekom Leistungsbeschreibung.	SAP: 04.08.2020 TSI: 26.08.2020	SAP: Deutsch TSI: Englisch

4.	Technische Beschreibung der Komponenten:					
	(a) Technische Beschreibung aller Komponenten, Systemanforderungen (OS, Datenbanken, etc.) inkl. technischer Kommunikationsbeziehungen/Schnittstellen	SAP/TSI	Der Leistungsteil der SAP ist über die Unterpunkte b) und c) dargestellt	Der Leistungsteil der Telekom ist über den Unterpunkt d) (Verification Components) dargestellt	veröffentlicht	Englisch
	(b) Frontend-Architektur	SAP	Architektur-Dokument IOS (GitHub): https://github.com/corona-wam-app/cwa-app-ios/blob/develop/docs/architecture-overview.md Architektur-Dokument Android (GitHub): https://github.com/corona-wam-app/cwa-app-android/blob/master/docs/architecture-overview.md	Keine	veröffentlicht	Englisch
	(c) CWA-Server-Architektur	SAP	Architektur-Dokument CWA Server (GitHub): https://github.com/corona-wam-app/cwa-server/blob/master/docs/architecture-overview.md	Keine	veröffentlicht	Englisch
	(d) Verification Components	TSI	Keine	Siehe Unterpunkt 2	veröffentlicht	Englisch
5.	Funktionale Kommunikationsbeschreibung: Beschreibung aller Kommunikationsbeziehungen (funktional) inkl. Schnittstellen-Spezifikationen	SAP	Architektur-Dokument (GitHub): https://github.com/corona-wam-app/cwa-documentation/blob/master/solution_architecture.md		veröffentlicht	Englisch
6.	Dokumentation und Quellcode für Drittparteien: Bei selbstentwickelten Produkten: Quellcode und zugehörige Dokumentation) inkl. Coding-Guidelines	SAP/TSI	IOS-App (GitHub): https://github.com/corona-wam-app/cwa-app-ios Android-App (GitHub): https://github.com/corona-wam-app/cwa-app-android CWA Server (GitHub): https://github.com/corona-wam-app/cwa-server	https://github.com/corona-wam-app/cwa-verification-server https://github.com/corona-wam-app/cwa-verification-portal https://github.com/corona-wam-app/cwa-verification-lam https://github.com/corona-wam-app/cwa-testresult-server	veröffentlicht	Englisch

Unterschriftenfassung

7.	Sicherheitskonzepte für alle Komponenten	SAP/TSI	Sicherheitsdokumentation SAP	Sicherheitskonzepte für die Einzelkomponenten gemäß Telekom Leistungsbeschreibung.	SAP: 08.06.2020 TSI: 29.07.2020	SAP: Englisch TSI: Deutsch
8.	Sicherheitskonzept für das Gesamtsystem	TSI	Zulieferung zum Sicherheitskonzept	Sicherheitskonzept gemäß Telekom Leistungsbeschreibung	31.12.2020	Deutsch
9.	Datenschutzkonzept für das Gesamtsystem inkl. Selbstauskunft über DSGVO-Compliance	SAP/TSI	Datenschutzkonzept Mobile Datenschutzkonzept CWA Server	Das Datenschutzkonzept gemäß Telekom Leistungsbeschreibung, außer für die Hotline, wird bis zum 03.06.2020 erstellt. Für die Hotline wird das Datenschutzkonzept bis zum 10.06.2020 erstellt.	SAP: 03.06.2020 TSI: 03.06.2020 TSI Hotline: 10.06.2020	Deutsch
10.	Datenschutz-Folgenabschätzung für das Gesamtsystem	TSI	Keine	Datenschutz-Folgenabschätzung gemäß Telekom Leistungsbeschreibung	07.06.2020	Deutsch
11.	Rechts- und Rollenkonzept/Berechtigungskonzept	TSI	Keine	Rechts- und Rollenkonzept gemäß Telekom Leistungsbeschreibung	29.07.2020	Deutsch
12.	Ergebnisse und Protokolle der Tests gemäß Testkonzept. (inkl. Zusammenfassung der Testergebnisse mit Benennung der Testabdeckungsquote, Beschreibung der Testfälle und der Testschritte)	SAP/TSI	Panel Test	UAT Test Testprotokolle als html-Export aus Jira/X-Ray gemäß Telekom Leistungsbeschreibung bei Bedarf auch als PDF- oder Excel-Export	SAP Panel Test: 05.06.2020 TSI: UAT Test, Testprotokolle 11.06.2020	Deutsch
13.	Ergebnis Langzeittest der Löschung auf iOS/Android Ebene	TSI	Keine	Ergebnis Langzeittest der Löschung auf iOS/Android Ebene	28.06.2020	Deutsch
14.	Testkonzept (High-Level-Dokument)	TSI	Keine	Testkonzept	06.06.2020	Deutsch
15.	Testat/Zertifikate (C5 Testat, ISO 27001 Zertifikat RZ Betrieb)	TSI	Keine	C5 Testat ISO 27001 Zertifikat	06.06.2020	Deutsch
16.	Testat Barrierefreiheit gem. Anlage 5	SAP	Testat Barrierefreiheit für iOS-App Testat Barrierefreiheit für Android-App	Keine	12.06.2020, 11:00 Uhr	Deutsch
17.	Allgemeines Wiederherstellungskonzept als Teil des Betriebshandbuchs	TSI	Keine	Siehe Unterpunkt 3	28.06.2020	Englisch
18.	Nachweis, dass App in den Stores akzeptiert wurde	SAP	Nachweis für iOS-App Nachweis für Android-App	Keine	14.06.2020	Englisch
19.	Bestätigung von Apple/Google zur Löschung	SAP	Nachweis Apple Nachweis Google	Keine	05.06.2020	Apple: Englisch Google: Deutsch

Unterschriftsfassung

20.	Referenz tatsächlich zu testender Geräte Modelle (inkl. gezeigter OS-Versionen)	TSI	Keine	Referenzliste Geräte Modelle	08.08.2020	Deutsch
-----	---	-----	-------	------------------------------	------------	---------

* * *

**ANLAGE 5
ABNAHMEKRITERIEN UND -PRÜFUNGEN**



**Bundesministerium
für Gesundheit**

Version 1.8

**Corona-Warn-App
Inbetriebnahme- und
Abnahmekriterien,
Prüfungen**

Informationen zum vorliegenden Dokument

Projekt/Auftrag	Corona-Warn-App
Dokumententitel	
Version	Version 1.8
Verantwortlicher Autor	Multiprojektmanagement Referat 512 (ext. Dienstleister Capgemini)
erstellt am	von
zuletzt bearbeitet am	05.08.2020 von
QS-geprüft am	von
Fertig gestellt am	von
Bearbeitungszustand	x In Bearbeitung vorgelegt fertig gestellt

Allgemeine Informationen

Ablage	
Aktenzeichen	
Auftragskennzeichen	
Veröffentlichung	Version am
Veröffentlichungsform	PDF
Review-Zyklus	entfällt
Kontakt	Bundesministerium für Gesundheit (BMG)
Organisationseinheit	Abteilung 5

Änderungsverzeichnis

<u>Version</u>	<u>Datum</u>	<u>Änderungen (Kapitel, Inhalt)</u>	<u>Bearbeitet von</u>	<u>Neuer Bearbeitungs- zustand</u>
0.0	13.05.2020	Initiale Anlage der Multiprojekt-Vorlage auf Grundlage V-Modell XT Bund / ITZBund	Multiprojektmanagement Office	akzeptiert
0.1	14.05.2020	Dokumentenstruktur vereinheitlichen	Multiprojektmanagement Office	akzeptiert
0.2	15.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.3	15.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.4	15.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.5	19.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.6	20.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.71	25.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.72	25.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.8	25.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
0.9	27.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
1.0	28.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
1.1	29.05.2020	Projektmanagement-Qualitätssicherung und -anpassungen	Multiprojektmanagement Office	akzeptiert
1.2	04.06.2020	Übergreifend	BMG	vorgelegt

1.3. - 1.8	05.08.2020	Übergreifend	BMG	vorgelegt
------------	------------	--------------	-----	-----------

Prüfverzeichnis

Die folgende Tabelle zeigt einen Überblick über alle Prüfungen - sowohl Eigenprüfungen wie auch Prüfungen durch eigenständige Qualitätssicherung - des vorliegenden Dokumentes.

Geprüfte Version	Datum	Anmerkungen	Prüfer	Anmerkungen
0.4	18.05.2020	alle Kapitel	BMG	(mündlich übermittelt)
0.6	20.05.2020	alle Kapitel	BMG	(schriftlich übermittelt)
0.71	25.05.2020	alle Kapitel	BMG	(mündlich übermittelt)
0.72	25.05.2020	alle Kapitel	BMG	(mündlich übermittelt)
0.8	25.05.2020	alle Kapitel	BMG	(schriftlich übermittelt)
0.9	27.05.2020	alle Kapitel	BMG	(schriftlich übermittelt)
1.0	28.05.2020	alle Kapitel	BMG	(schriftlich übermittelt)
1.1	29.05.2020	alle Kapitel	BMG	akzeptiert (Version 1.1)
1.8	05.08.2020	alle Kapitel	BMG	akzeptiert

Inhaltsverzeichnis

1.	Einleitung und Zielsetzung dieses Leitfadens	7
	Die Qualitäts-Dimensionen des ISO-Standards 25010	7
	Organisatorischer und technischer Rahmen	8
	Auswirkung von Mängeln auf die Go-Live-Freigabe und Abnahme.....	8
2.	Prüfobjekt und Abgrenzung	10
	Übersicht Systemlandschaft und Glossar.....	11
3.	Prüfstrategie.....	11
4.	Prüfvorgehen und Ableitung der Prüffälle	12
4.1	Prüfvorgehen.....	12
	Prüfchema	12
	Abdeckung	12
4.2	Ableitung der Prüffälle	13
	„Übersicht der Epics“ (gem. Github)	13
	Nutzer-Prozessphasen (gem. Github)	14
	Support-Prozesse (gem. Github)	14
5.	Prüffälle	15
5.1	Prüffälle aus User Stories und Ableitung aus bestehender Dokumentation	15
	Prüffall-Matrix zu den User Stories:	15
5.1.1	Anbahnung und Installation (Onboarding-Prozess)	17
5.1.2	Informationen und Instruktionen zur Nutzung der Applikation.....	20
5.1.3	Nutzung im Regelprozess	21
5.1.4	Kontaktfall (Begegnung mit infizierter Person)	26
5.1.5	Covid-19-Testergebnismeldung.....	29
5.1.6	Auslösen einer Warnung.....	32
5.1.7	Parametrisierung	36
5.1.8	Technische Unterstützung.....	37
5.1.9	Barrierefreiheit	37
5.1.10	Content Management.....	37
5.2	Prüffälle aus allgemeinen Qualitätskriterien.....	38
5.2.1	Portabilität nach ISO25010.....	39
5.2.2	Usability nach ISO25010	39
5.2.3	Sicherheit nach ISO25010	40
5.2.4	Performanz nach ISO25010.....	40
5.2.5	Zuverlässigkeit nach ISO25010.....	41
5.2.6	Funktionale Eignung nach ISO25010	44

5.2.7 Kompatibilität nach ISO25010.....	44
5.2.8 Wartbarkeit nach ISO25010	44
5.3 Prüffälle: Anforderungen aus App-Plattform Guidelines	46
UX-Standards	46
Anforderungen an den Entwicklungsprozess	46
App Store	46
5.2 Prüffälle aus Anforderungen der Informationssicherheit und des Datenschutzes	47
5.3 Prüffälle aus Anforderungen der Barrierefreiheit.....	48
6. Ergebnisdokumentation.....	48
- Test-Konzept (z.B. Word, Übergabe PDF/A)	48
- Test-Protokoll (z.B. Excel oder Tool-Export, Übergabe PDF/A).....	48
- Test-Bericht (z.B. Word, Übergabe PDF/A).....	48
- Ergebnis-Präsentation (z.B. PowerPoint, Übergabe PDF/A)	48
Glossar	49
Abbildungsverzeichnis	51
Anhang	52
Übersicht der User Stories (Stand 14.05.2020)	52

1. Einleitung und Zielsetzung dieses Leitfadens

Dieses Dokument basiert auf dem Informations- und Sachstand des 27. Mai 2020.

Das vorliegende Dokument soll das Vorgehen zur Prüfung der Lieferung der Corona-Warn-App erläutern.

Dazu beschreibt der vorliegende Leitfaden in Ergänzung zu den vertraglichen Regelungen, welche Dokumente und Artefakte zur Prüfung des Vorliegens der vereinbarten Ergebnisse herangezogen werden sollen und **WAS** anhand dessen geprüft werden soll. Das vorliegende Dokument beschreibt nicht **WIE** der konkrete Test der Anwendung durch die Industriepartner während der Software-Entwicklung und bis zum produktionsreifen Stand „Bereit zur Inbetriebnahme“ erfolgen soll. Die Industriepartner müssen hierfür Testprotokolle, Kennzahlen und Konzepte vorlegen, um nachzuweisen, dass sowohl funktionale als auch nicht funktionale Anforderungen in angemessener Qualität implementiert worden sind.

Aufgrund der Tragweite und der Mengengerüste, sollten die nachfolgend beschriebenen Qualitätsprinzipien dienstleistersseitig vor Produktivsetzung mit entsprechender Test-Abdeckung (produktionsreif) streng gehandhabt werden, aber auch auftraggebersseitig bei der Abnahmeentscheidung. Hilfweise kann von der vorgesehenen Nachweisart nach vorheriger Abstimmung mit dem Auftraggeber abgewichen werden, wenn alternative Nachweis- und Belegarten von gleicher Wirksamkeit vereinbart werden.

Zur Erläuterung und Abgrenzung referenziert dieses Dokument stellenweise einzelne Systemkomponenten der Corona-Warn-App Systemlandschaft, diese sind im Glossar inklusive Schaubild und Beschreibung aufgeführt.

Die Qualitäts-Dimensionen des ISO-Standards 25010

Die Prüfung orientiert sich an den Qualitätseigenschaften für Software gemäß ISO25010 (Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and Software Quality Models), siehe folgende Abbildung. Die Aspekte zum Thema Betrieb sind von der Betrachtung in diesem Dokument jedoch ausgeklammert.

Kompatibilität		Funktionale Eignung			Wirtschaftlichkeit		
Interoperabilität Wie gut können zwei oder mehr Systeme interagieren, z.B. Daten austauschen und nutzen?	Ko-Existenz Wie gut funktionieren die Software, wenn sie mit anderen Softwareprodukten auf der gleichen Umgebung läuft?	Funktionale Korrektheit Funktioniert die Software wie gewünscht / spezifiziert?	Funktionale Vollständigkeit Wie viele der benötigten Funktionen werden wirklich von der Software abgebildet?	Funktionale Angemessenheit Erfüllt die Software die Anforderungen oder gibt es auch überflüssige/nicht benötigte Funktionen?	Testbarkeit Können Tests für das System durchgeführt werden, um sicherzustellen, dass die Funktionalität ist (korrekt)?	Modularität Hochwertiges System aus unterschiedlichen Komponenten, welche die Flexibilität erhöhen? (Erweiterung) geändert werden können?	Änderbarkeit Kann die Software ohne große (Erweiterung) Änderungen angepasst und geändert werden?
Portabilität		Zuverlässigkeit			Wieder- verwendung Können Teile des Systems für die Entwicklung anderer Systeme wiederverwendet werden?	Analysierbarkeit Unterstützt die Software die Diagnose von Fehlfunktionen? Können Konzepte sowie Änderungen eingetragener werden?	
Austauschbarkeit Kann die Software durch eine andere mit der gleichen Funktionalität ausgetauscht werden?	Adaptability Kann die Software auch auf anderen Hardware oder Betriebssystemen eingesetzt werden? Ist es möglich auf neue Versionen von Betriebssystemen etc. zu migrieren?	Recoverability Kann die Software nach einem Problem durch einen Host/Host ohne Datenverlust weiterarbeiten?	Fehlertoleranz Wie gut toleriert die Software im Falle von Host- oder Software-Ausfällen?				
Installierbarkeit Kann die Software ohne Probleme installiert, konfiguriert und Updates eingespielt werden?		Reife Wie stabil und fehlerfrei arbeitet die Software unter Normalbedingungen?	Verfügbarkeit Ist die Software im gewünschten Maße nutzbar – Stichwort SLA/SL?		Usability		
Performance Effizienz		Sicherheit			User Interface Ästhetik Ist das UI für den Benutzer attraktiv und empfehlend?	Appropriateness recognizability Ist es für den Benutzer erkennbar, ob die systeme seine Anforderungen erfüllt?	
Zeitverhalten Wie sind die Antwortzeiten des Systems bei Requests um die zu verarbeiten und eine Antwort zu senden?	Kapazität Wie viele Benutzer können mit dem System zur gleichen Zeit arbeiten? Ist die Speicher-Kapazität auch für die Zukunft ausreichend?	Nachweisbarkeit Ist der interne Programmablauf nach der Ausführung nachvollziehbar?	Vertraulichkeit Ist der Zugriff auf Daten in der Software nur für die autorisierten Benutzer möglich?	Account-ability Ist hoch verfügbar, wie in dem System welche Funktionen ausgeführt sind?	Benutzerfehler-Vermeidung Wurde das System vorausschauend designed, um Benutzerfehler von vornherein zu vermeiden?	Eriernbarkeit Wie schnell und wie oft kann ein Benutzer lernen, mit dem System umzugehen?	
Ressourcenverbrauch Ist die Art und Menge von benötigten Ressourcen wie erwartet?		Integrität Ist die Software geschützt gegen unautorisierten Zugriff z.B. durch Malware oder Zugriff?	Authentizität Ist jede Person / Programm, die auf das System zugreift, auch werlich die, für die sie sich ausgibt?		Verwendbarkeit Ist das System einfach zu verwenden? Erlaubt es die Benutzer-Erweiterungen in der Verwendung?	Barrierefreiheit Kann das System auch von Benutzern mit Behinderungen effektiv genutzt werden?	

Abbildung 1: Qualitäts-Dimensionen des ISO-Standards 25010

Organisatorischer und technischer Rahmen

Der organisatorische und technische Rahmen wird vom Vertrag definiert. Daraus sich ergebende Randbedingungen werden als nicht-funktionale Anforderungen in die Prüffälle integriert.

Auswirkung von Mängeln auf die Go-Live-Freigabe und Abnahme

Grundsätzlich wird davon ausgegangen, dass eine Software auch Mängel oder Fehler enthält. Um diese zu finden, werden dienstleisterseitig Tests mit angemessener Abdeckung durchgeführt, bis der Reifegrad „bereit zur Inbetriebnahme“ (produktionsreif) erreicht ist.

Betriebsbehindernde Mängel verhindern die Inbetriebnahme. Ein betriebsbehindernder Mangel liegt auch vor, wenn die leichten Mängel in Summe insgesamt zu einer nicht unerheblichen Einschränkung der Nutzung einer vertraglichen Leistung führen.

Die Inbetriebnahme kann erfolgen, auch wenn eine überschaubare Zahl von leichten Fehlern vorliegt.

Erhebliche Fehler verhindern die Inbetriebnahme, wenn kein operativer Workaround besteht und diese nicht zum Produktivstart zu beheben sind.

Mängel der Kategorie „Blocker“ sind Inbetriebnahme- und abnahmeverhindernd.

Fehler werden systematisch erfasst und auch kategorisiert:

Kategorie	Beschreibung (EVB-IT)	Fehlerklasse gem. „High-Level-Testplan“ T-Systems (20.05.2020)
Leicht	Ein leichter Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung ohne oder mit unwesentlichen Einschränkungen möglich ist.	Fehlerklasse 3: Die zweckmäßige bzw. wirtschaftlich sinnvolle Nutzung des Gesamtsystems ist gemäß Leistungsbeschreibung nur unwesentlich, das heißt ohne nennenswerte Auswirkungen auf die Funktionalität des Gesamtsystems eingeschränkt bzw. behindert (beispielhafter Mangel: das Testergebnis für einen App-Nutzer wird zwar inhaltlich richtig angezeigt, jedoch in einem unschönen falschen Format).
Erheblich	Ein betriebsbehindernder Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung erheblich eingeschränkt ist.	Fehlerklasse 2: Die zweckmäßige bzw. wirtschaftlich sinnvolle Nutzung des Gesamtsystems ist gemäß Leistungsbeschreibung erheblich eingeschränkt bzw. behindert. Die Kernfunktionalität ist gewährleistet, es liegt jedoch ein gravierender Fehler in einer wesentlichen Teilfunktionalität vor, der das Arbeiten erheblich behindert oder unzumutbar macht (beispielhafter Mangel: Das Testergebnis für einen App-Nutzer wird inhaltlich zwar korrekt angezeigt, wichtige Empfehlungen aufgrund des Testergebnisses werden jedoch für den App-Nutzer nicht vollständig angezeigt).
Blocker	Ein betriebsverhindernder Mangel liegt vor, wenn die Nutzung einer vertraglichen Leistung unmöglich oder schwerwiegend eingeschränkt ist.	Fehlerklasse 1: Die zweckmäßige bzw. wirtschaftlich sinnvolle Nutzung des Gesamtsystems gemäß Leistungsbeschreibung ist nicht möglich oder durch Nicht- oder Fehlfunktion(en) von Programmen, Modulen oder Komponenten so eingeschränkt bzw. behindert, dass die Abwicklung des Tagesgeschäftes nicht zumutbar fortgeführt bzw. ein Abnahmetest nicht sinnvoll fortgeführt werden kann (beispielhafter Mangel: Das Testergebnis für einen App-Nutzer wird falsch angezeigt).

Abbildung 2: Tabelle der Fehler-Kategorien

2. Prüfobjekt und Abgrenzung

Ziel der Corona-Warn-App ist es, SARS-CoV-2-Infektionsketten schnellstmöglich zu erkennen und zu durchbrechen. Nutzer sollen zuverlässig und schnell über Begegnungen mit infizierten Nutzern der App und damit mögliche Übertragungen des Virus informiert werden, damit sie sich freiwillig isolieren können, um damit zu einer Eindämmung der SARS-CoV-2-Pandemie beizutragen.

Folgende Prüfobjekte sind in Scope:

- **App:**
 - Wenn die App nativ für Android und iOS entwickelt wird:
 - Corona-Warn-App für Android als installierbare .apk Datei inkl. korrelierendem Quellcode im Github und Build-Skripte zur Erstellung der .apk Datei jeweils in der Version „Bereit zur Inbetriebnahme“ bereitzustellen durch die Softwaredienstleister
 - Corona-Warn-App für iOS als installierbare .ipa Datei inkl. korrelierendem Quellcode im Github und Build-Skripten zur Erstellung der .ipa Datei jeweils in der Version „Bereit zur Inbetriebnahme“ bereitzustellen durch die Softwaredienstleister
- **Backend:**
 - Schnittstellenspezifikation für alle relevanten Schnittstellen der App und angrenzenden Systemen in der Version „Bereit zur Inbetriebnahme“ bereitzustellen durch die Softwaredienstleister
 - API Keys und Zugriffsdaten bereitzustellen durch die Softwaredienstleister mindestens auf einer Pre-Live-Test-Umgebung für aussagekräftige Last- und Performanztests
 - Quellcode im Github und Build-Skripte für alle relevanten Backend-Komponenten, die Daten der App verarbeiten oder zuliefern (z.B. Portal-Server) inkl. Deploy-Artefakten, z.B. „war“-Datei für das Backend in der Version „Bereit zur Inbetriebnahme“ bereitzustellen durch die Softwaredienstleister.
 - App und Backend 3rd Party Bibliotheken/Listen:
 - alte Versionen – Security Vulnerabilities, Lizenzen (Open Source?)
 - Fachliche Bewertung der Datenkritikalität (eigene App darf nur an eigene Daten kommen)
 - Lösung-Architektur-Beschreibung des Backends passend zur Auslieferung „Bereit zur Inbetriebnahme“ bereitzustellen durch die Softwaredienstleister

Siehe auch Github (Link vom 19.05.2020):

- <https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/README.de.md>
- https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/scoping_document.de.md

Übersicht Systemlandschaft und Glossar

Eine Gesamtübersicht der geplanten Systemlandschaft der Corona-Warn-App findet sich im Anhang dieses Dokuments (siehe Abbildung 5, Stand 27.05.2020). Einzelne in diesem Dokument in den User Stories oder Prüffällen referenzierte Systemkomponenten sind zur Erläuterung des Gesamtprozesses im Glossar am Ende des Dokuments beschrieben (siehe Glossar, auf Grundlage der Veröffentlichung im GitHub, Stand 27.05.2020).

3. Prüfstrategie

Die Prüfstrategie erstreckt sich auf:

- die Verwendung des Lieferobjekts App
- die in der Datenverarbeitung der App beteiligten Backend-Systeme, Schnittstellen und 3rd Party-Bibliotheken
- die Prüfung von Anforderungen im Kontext der im GitHub veröffentlichten Beschreibungen (Stand: 19.05.2020)
- die Prüfung gegen einschlägige Kriterien aus Industriestandards
- die Prüfung gegen Akzeptanzanforderungen aus dem gesellschaftlichen und Experten-Diskurs zur Corona-Warn-App.

Die Prüfstrategie erstreckt sich nicht auf:

- den Entwicklungsprozess der Entwicklungsdienstleister
- das Testkonzept und die Testdurchführung
- die Inbetriebnahme, Betrieb und Weiterentwicklung von Lieferobjekten im gemeinsamen Wirkbetrieb von: App, Portal-Server, Labor-Informationssystem (LIS)
- Anforderungen an die Betriebsumgebung und den Betrieb (diese werden vertraglich spezifiziert).

4. Prüfverfahren und Ableitung der Prüffälle

4.1 Prüfverfahren

Die Prüfstrategie (siehe oben) verdeutlicht die große Heterogenität der Anforderungen. Um die Vergleichbarkeit der zu prüfenden Aspekte in mess- und vergleichbare Prüffälle zu erreichen, werden alle Prüfpunkte nach dem folgenden Schema dargestellt:

Prüfschema

- **ID:** [eindeutige Zuordnung]
- **Prüfpunkt:** Was wird geprüft?
- **Prüfverfahren:** Wie wird geprüft?
- **Nachweis / Ergebnistyp:** Wie wird der Nachweis erbracht?

Als Darstellung dafür wird die folgende tabellarische Struktur verwendet:

ID	Prüfpunkt	Prüfverfahren	Nachweis / Ergebnistyp
	<i>Bsp.: Anwendung muss barrierefrei sein</i>	<i>Bsp.: Prüfung gegen BIT-V Kriterien</i>	<i>Bsp.: Ergebnisprotokoll Dienstleister als Nachweis</i>

Abbildung 3: Tabellarisches Prüfschema

Abdeckung

Wenn in diesem Dokument im Prüfverfahren von „Nutzer“ gesprochen wird, dann ist bei der Prüfung im entwicklerseitigen Testkonzept und Testprotokoll des Dienstleisters die Abdeckung darzustellen und nachzuweisen für:

- abgedeckte Betriebssystem-Vollversionen sowie Abwärts-Kompatibilitätsspanne
- abgedeckte Hersteller-Endgerätemodelle
- ggfs. abgedeckte Browser-Versionen.

Mit dem gewählten Vorgehen werden als spezifische Anpassung die klassischen Anforderungsdimensionen mit zwei Mitteln abgedeckt:

- Vertrag
- Kapitel 5 dieses Prüf-Leitfadens (Prüffälle).

Die klassischen Anforderungs-Dimensionen sind:

- **Funktionale Anforderungen**
 - (zu jedem Akzeptanzkriterium ist mind. ein funktionaler Test nachzuweisen)
- **Nicht-Funktionale Anforderungen**
 - **Funktionalität**
Vorhandensein von Funktionen mit festgelegten Eigenschaften (z.B.: Angaben zu Genauigkeiten von berechneten Werten)

- **Zuverlässigkeit**
Fähigkeit, das Leistungslevel unter festgelegten Bedingungen über einen festgelegten Zeitraum zu bewahren
(z.B.: Angaben zur Verfügbarkeit oder zur Wiederherstellbarkeit nach Ausfällen hinsichtlich Aufwand und Zeit)
- **Benutzbarkeit**
Eigenschaften, die zur Benutzung erforderlich
(z.B. Verständlichkeit, Erlernbarkeit und Bedienbarkeit)
- **Effizienz**
Performanceanforderungen sowie Anforderungen zum Verbraucherverhalten beim Betrieb
- **Änderbarkeit**
Erforderlicher Aufwand, um Änderungen an der Software vorzunehmen
(z.B.: Korrekturen, Verbesserungen oder geänderte Anforderungen)
- **Übertragbarkeit**
Migrationsfähigkeit und Festigkeit
(z.B. organisatorische Umgebung, andere Hardware- oder Softwareumgebung)
- **Randbedingungen**
Bedingungen und Einschränkungen, die sich aus dem organisatorischen und technischen Rahmen ergeben
(z.B. Gesetze, Verordnungen, Richtlinien, einzuhaltende Standards, technologische Vorgaben wie Hardware- oder Software-Plattformen oder zwingend einzuhaltende Terminvorgaben)

4.2 Ableitung der Prüffälle

Die übergreifenden Funktionalitäten im gesamten Prozess sowie die einzelnen Kontakt-Ereignisse, welche für die Nutzung und Akzeptanz der App erforderlich sind, wurden in sogenannten „Epics“ beschrieben.

Da diese Epics der Anforderungsrahmen für die nachfolgend entwickelten fachlichen und technischen Beschreibungen des Zielzustands der App, der sogenannten „User Stories“, sind, werden im Folgenden diese (in der agilen Softwareentwicklung üblichen Spezifikationen von Anforderungen) in Form der Beschreibungen auf der Internetseite github mit Stand vom 14.05.2020 (ca. 19:00 Uhr) wiedergegeben.¹

„Übersicht der Epics“ (gem. Github)

¹ Quelle: https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/scoping_document.de.md#%C3%BCbersicht-der-epics
abgerufen am 14.05.2020

„Die Funktionen der Applikation sind in Nutzer-Prozessphasen (mit direktem Bezug zur User Journey) und übergreifende Unterstützungsprozesse unterteilt. Eine Übersicht der Epics ist nachfolgend dargestellt:

Nutzer-Prozessphasen (gem. Github)

#	Epic	Beschreibung
1	Anbahnung und Installation (Onboarding-Prozess)	Sämtliche Prozesse, die insbesondere bei erstmaliger Nutzung der Applikation erfolgen (z.B. Zustimmung Datenschutz, Sprachauswahl)
2	Informationen und Instruktionen zur Nutzung der Applikation	Hilfestellungen zur Nutzung der Applikation (z.B. Benutzerhandbuch, Tutorial) sowie Informationen zum Impressum der Applikation.
3	Nutzung im Regelprozess	Funktionen der Applikation im "idle mode" (z.B. Aktivierung/Deaktivierung, Anpassung von Einstellungen, Überwachung von App-Aktivität)
4	Kontaktfall (Begegnung mit infizierter Person)	Beinhaltet alle Funktionen rund um Kontaktpunkte (z.B. Benachrichtigungen, Handlungsempfehlungen)
5	Covid-19-Testergebnismeldung	Funktionen im Zusammenhang mit der Testergebnismeldung
6	Auslösung einer Warnung	Prozess zur Auslösung einer Warnung im Falle eines positiven Testergebnisses

Support-Prozesse (gem. Github)

#	Epic	Beschreibung
7	Parametrisierung	Parameter der Kontaktpunktdefinition
8	Technische Unterstützung	Support-Prozesse (z.B. Hotlines)
9	Barrierefreiheit	Die Apps von Trägern öffentlicher Gewalt müssen dem Behindertengleichstellungsgesetz (BGG) nach barrierefrei sein (§ 12). Apps sollen von allen Menschen mit Behinderungen bedient werden können.
10	Content-Management	Zur Anpassung und Aktualisierung von Inhalten in der Applikation (Texte, Links, Hotlines etc.)

5. Prüffälle

5.1 Prüffälle aus User Stories und Ableitung aus bestehender Dokumentation

Die Anforderungen an die Corona-Warn-App, die den fachlichen Umfang der Anwendung definieren, wurden in der üblichen Form von sogenannten „User Stories“ aus Nutzersicht formuliert und finden sich am Ende bzw. im Anhang dieses Dokumentes.

Die Prüffälle aus diesen User Stories decken aus fachlicher Perspektive sowohl Prüfkriterien für die mobile Applikation als auch für das Backend und den Portal-Server (Gesundheitsämter, RKI, Hotline) und das Labor-Informationssystem LIS (Ärzte) ab.

Insbesondere stellt die Prüfung von Anforderungen, die sowohl Backend- als auch Frontend-Komponenten einbeziehen, die Funktionalität über verschiedene Stakeholder und Applikationsbausteine hinweg sicher (Ende-zu-Ende). Ergänzende, im Zuge der Erstellung dieses Dokuments abgeleitete Prüffälle werden mit dem Bezeichnungszusatz „A“ für Ableitung jeweils im zugehörigen Abschnitt mit aufgeführt.

Folgend eine Übersicht, welche die vorhandenen User Stories klassifiziert (Stand 19.05.2020).

Prüffall-Matrix zu den User Stories:

Nutzer & Plattform		Mobile Applikation (Corona Warn App)	Ende-zu-Ende (Mobile Applikation und Backend / CMS)	Backend / CMS
Querschnittlich integriert:	App-Nutzer (App)	<u>E01.01 - E01.07</u> <u>E01.A1</u> <u>E02.01 - E02.06</u> <u>E03.01 + E03.03</u> <u>E03.A1 - E03.A2</u> <u>E08.01</u> <u>E09.01 - E09.02</u>	<u>E03.02</u> <u>E04.01 - E04.02</u> <u>E05.01 - E05.02</u> <u>E06.01 - E06.03</u> <u>E06.05 - E06.06</u>	<u>E09.03</u>
	Gesundheitsämter (Portal-Server oder LIS)		<u>E04.A2</u> <u>E06.04 (1/2)</u>	<u>E04.A1</u>
	RKI (Portal-Server)		<u>E07.01</u> <u>E07.A1</u>	<u>E10.01</u>

Hotline (Portal-Server) <i>keine med. oder psychologische Beratung, nur Beantwortung von festgelegten Standard- Informationen)</i>		<u>E06.04 (2/2)</u>	<u>E02.A1 – E02.A2</u>
Ärzte (Labor Informations System - LIS)			<u>E05.A1 – E05.A2</u>
Querschnittlich integriert: Verifikations-Server (genutzt von CWA, CWA-Server, LIS, Portal-Server)			

Abbildung 4: Matrix der Prüffälle aus den User Stories

Aus diesen Anforderungen ergeben sich die nachstehenden Prüfpunkte. Die Prüfpunkte können durch das beschriebene Prüfverfahren verifiziert werden und sollen in einem Testprotokoll kodifiziert werden. Nur so kann sichergestellt werden, dass die Software in einer Version vorliegt, die in der Lage ist, die Bedürfnisse der Nutzergruppen befriedigen zu können.

5.1.1 Anbahnung und Installation (Onboarding-Prozess)

Prüf-ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E01.01	Eine Einführung in die Funktionsweise der App wird angezeigt.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll
	E01.01	Eine Einführung in die Funktionsweise der App wird bei weiteren Startvorgängen nicht angezeigt.	Ein App-Nutzer startet die Applikation ein weiteres Mal.	Vorlage Testprotokoll
	E01.01	Die erklärenden Inhalte sind in den jeweiligen Funktionsbereichen für den App-Nutzer vorhanden.	Ein App-Nutzer startet die Applikation ein weiteres Mal und öffnet die Funktionsbereiche der App.	Vorlage Testprotokoll
	E01.02	Die Nutzungsbedingungen und Datenschutzbestimmungen werden angezeigt.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll
	E01.02	Die tatsächliche Nutzung der App ist erst möglich, wenn den Nutzungsbedingungen und Datenschutzbestimmungen zugestimmt werden.	Ein App-Nutzer startet die Applikation erstmalig und versucht, die Zustimmung zu den Nutzungsbedingungen und Datenschutzbestimmungen zu umgehen.	Vorlage Testprotokoll
	E01.02	Die Nutzungsbedingungen und Datenschutzbestimmungen werden so lange stets beim Start der App angezeigt, bis der Nutzer zugestimmt hat.	Ein App-Nutzer startet die Applikation ein weiteres Mal.	Vorlage Testprotokoll
	E01.02	Es ist möglich, den Nutzungsbedingungen und Datenschutzbestimmungen zuzustimmen.	Ein App-Nutzer startet die Applikation erstmalig und stimmt den Nutzungsbedingungen und Datenschutzbestimmungen zu.	Vorlage Testprotokoll
	E01.02	Die Nutzungsbedingungen und Datenschutzbestimmungen sind in der App einsehbar.	Ein App-Nutzer startet die Applikation ein weiteres Mal und ruft die Nutzungsbedingungen und Datenschutzbestimmungen in der App auf.	Vorlage Testprotokoll
	E01.02	Die Nutzungsbedingungen und Datenschutzbestimmungen werden bei weiteren Startvorgängen nicht angezeigt.	Ein App-Nutzer startet die Applikation ein weiteres Mal.	Vorlage Testprotokoll
	E01.03	Der App-Nutzer wird bei erstmaliger Nutzung der Applikation gefragt, ob er der Erstellung pseudonymer IDs und deren Aussendung an Geräte in seiner Nähe durch die App zustimmt.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll

E01.03	Der App-Nutzer wird bei weiteren Nutzungen der Applikation nicht erneut gefragt, ob er der Erstellung pseudonymer IDs und deren Aussendung an Geräte in seiner Nähe durch die App zustimmt.	Ein App-Nutzer startet die Applikation weiteres Mal.	Vorlage Testprotokoll
E01.04	Der App-Nutzer wird bei erstmaliger Nutzung der Applikation gefragt, ob die Applikation die Tracing-Funktionalitäten nutzen darf, damit er die mobiltelefonseitige Nutzung der Applikation kontrollieren kann.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll
E01.04	Der App-Nutzer wird bei weiteren Nutzungen der Applikation nicht erneut gefragt, ob die Applikation die Tracing-Funktionalitäten nutzen darf, damit er die mobiltelefonseitige Nutzung der Applikation kontrollieren kann.	Ein App-Nutzer startet die Applikation weiteres Mal.	Vorlage Testprotokoll
E01.05	Der App-Nutzer wird bei erstmaliger Nutzung der Applikation gefragt, ob die Applikation ihm Benachrichtigungen (Mittellungen) schicken darf.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll
E01.05	Der App-Nutzer wird bei weiteren Nutzungen der Applikation nicht erneut gefragt, ob die Applikation ihm Benachrichtigungen (Mittellungen) schicken darf.	Ein App-Nutzer startet die Applikation weiteres Mal.	Vorlage Testprotokoll
E01.05	Der App-Nutzer wird bei erstmaliger Nutzung der Applikation gefragt, ob die eingestellte Systemsprache "Deutsch" von der App übernommen werden soll.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll
E01.05	Der App-Nutzer wird bei erstmaliger Nutzung der Applikation gefragt, ob die eingestellte Systemsprache "Englisch" von der App übernommen werden soll.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll
E01.05	Die Sprache der App (Content) ist Deutsch.	Ein App-Nutzer startet die Applikation nachdem er die	Vorlage Testprotokoll

		Sprache Deutsch ausgewählt hat.	
E01.05	Die Sprache der App (Content) ist Englisch.	Ein App-Nutzer startet die Applikation nachdem er die Sprache Englisch ausgewählt hat.	Vorlage Testprotokoll
E01.05	Der App-Nutzer wird bei weiteren Nutzungen der Applikation nicht erneut gefragt, ob die eingestellte Systemsprache von der App übernommen werden soll.	Ein App-Nutzer startet die Applikation weiteres Mal.	Vorlage Testprotokoll
E01.05	Sofern die eingestellte Systemsprache nicht im Content hinterlegt ist, sollte die Systemsprache "Englisch" (Default) von der App übernommen werden soll.	Ein App-Nutzer startet die Applikation erstmalig.	Vorlage Testprotokoll
E01.05	Der App-Nutzer sollte im Menü der App die Möglichkeit haben, seine Sprache zu wechseln.	Ein App-Nutzer startet die Applikation weiteres Mal und ändert im Menü die Sprache der App von Deutsch auf Englisch.	Vorlage Testprotokoll
E01.05	Der App-Nutzer, der im Menü der App die Sprache geändert hat, sollte die neu ausgewählte Sprache angezeigt bekommen.	1. Ein App-Nutzer startet die Applikation ein weiteres Mal, nachdem er im Menü die Sprache der App von Deutsch auf Englisch geändert hat. 2. Ein App-Nutzer startet die Applikation ein weiteres Mal, nachdem er im Menü die Sprache von Englisch zurück auf Deutsch geändert hat.	Vorlage Testprotokoll

Weitere abgeleitete Prüffälle zur Anbahnung und Installation (Kennzeichnung: Exx.Ay)

E01.A1 <u>(CCC)</u>	Für die Nutzung der App fallen keine App-seitigen Gebühren an.	<ul style="list-style-type: none"> - kostenloser Download (keine Store-seitigen Gebühren) - kostenlose Nutzung (keine In-App-Gebühren/Käufe) 	Entfällt
------------------------	--	--	----------

[Link zur Prüffall-Matrix!](#)

5.1.2 Informationen und Instruktionen zur Nutzung der Applikation

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E02.01	Der App-Nutzer soll Zugriff auf eine FAQ-Liste haben können.	Ein App-Nutzer startet die Applikation, öffnet das Applikationsmenü und gelangt über einen Link auf eine Internetseite oder einen integrierten Webview mit Informationen zur App (FAQ).	Vorlage Testprotokoll
	E02.02	Der App-Nutzer soll Zugriff auf eine Anleitung zur Applikation haben, um die Anwendung und ihre Funktionen zu verstehen.	Ein App-Nutzer startet die Applikation, öffnet das Applikationsmenü und gelangt über einen Link auf eine Internetseite, auf der die Anwendung und ihre Funktionen erklärt werden.	Vorlage Testprotokoll
	E02.02	Die Anleitung zur Applikation, welche die Anwendung und ihre Funktionen beschreibt, ist für einen Laien verständlich.	Ein "Laie" liest die Anleitung zur Applikation, welche die Anwendung und ihre Funktionen beschreibt.	Vorlage Testprotokoll
	E02.03	Die Anleitung zur Applikation, welche die Anwendung und ihre Funktionen beschreibt, enthält neben Text auch einen Verweis auf ein externes Erklärvideo mit vergleichbarem Inhalt – soweit vom Auftraggeber bereitgestellt.	Ein App-Nutzer startet die Applikation und öffnet das Applikationsmenü und gelangt über einen Link auf eine Internetseite, auf der die Anwendung und ihre Funktionen erklärt werden und findet dort auch ein Video und kann dieses Video dort starten und ansehen.	Vorlage Testprotokoll
	E02.04	Der App-Nutzer soll Zugriff auf ein Impressum der Applikation haben.	Ein App-Nutzer startet die Applikation, öffnet das Applikationsmenü und gelangt über einen Link auf das Impressum.	Vorlage Testprotokoll
	E02.04	Das Impressum der Applikation soll die üblichen Inhalte zur Impressumspflicht beinhalten, also bspw. wer für Entwicklung und Inhalte der Applikation verantwortlich ist.	Ein App-Nutzer startet die Applikation, öffnet das Applikationsmenü und gelangt über einen Link auf das Impressum und prüft es gegen §5 TMG.	Nachweis der TMG-Compliance erfolgt durch das RKI und ist nicht abnahmeverhindernd

E02.05	Der App-Nutzer kann jederzeit die Nutzungsbedingungen und Datenschutzinformation einsehen.	Ein App-Nutzer startet die Applikation, öffnet das Applikationsmenü und gelangt über einen Link auf Nutzungsbedingungen und Datenschutzinformationen.	Vorlage Testprotokoll
E02.06	Der App-Nutzer sollte verschiedene Hotlines angeboten bekommen zu technischen, datenschutzbezogenen, gesundheitsbezogenen und psychologischen Fragestellungen sowie zur Verifikation eines Testergebnisses.	Ein App-Nutzer startet die Applikation und öffnet das Applikationsmenü und gelangt über einen Link auf einen Bereich Hotlines.	Vorlage Testprotokoll
E02.06	Die Informationen zur Hotline sollten neben der Rufnummer sowie einer kurzen inhaltlichen Beschreibung des jeweiligen Dienstes auch die Anzeige der zeitlichen Erreichbarkeit der Hotlines (z.B.: 24/7) enthalten.	Ein App-Nutzer startet die Applikation und öffnet das Applikationsmenü und gelangt über einen Link auf einen Bereich Hotlines.	Vorlage Testprotokoll
E02.08	Die Hotlines sollten direkt aus der App angewählt werden können.	Ein App-Nutzer startet die Applikation und öffnet das Applikationsmenü und gelangt über einen Link auf einen Bereich Hotlines und startet aus der App einen Anruf über das Mobilfunknetz bzw. VoIP-Call ("normaler Anruf"?)	Vorlage Testprotokoll
		1.	

5.1.3 Nutzung im Regelprozess

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E03.01	Der App-Nutzer kann jederzeit die Applikation ausschalten	Ein App-Nutzer A startet die App. Der App-Nutzer hat Zugriff auf	Vorlage Testprotokoll

		(Bluetooth im Hintergrund und Hash-Generierung).	<p>einen "Ausschalter" und kann diesen aktivieren.</p> <p>Ein zweiter App-Nutzer B startet seine App. Beide stellen den Kontaktfall (siehe unten "Kontaktfall") nach. Der App-Nutzer B stellt eine positive Testergebnismeldung (siehe "Covid-19-Testergebnismeldung") nach.</p> <p>Der App-Nutzer A prüft, ob seine App eine Warnung erhält.</p>	
E03.01	Der App-Nutzer kann jederzeit die Applikation einschalten (Bluetooth im Hintergrund und Hashgenerierung).	<p>Ein App-Nutzer A startet die App. Der App-Nutzer hat Zugriff auf einen "Ausschalter" und kann diesen aktivieren.</p> <p>Ein zweiter App-Nutzer B startet seine App. Beide stellen den Kontaktfall (siehe unten "Kontaktfall") nach. Der App-Nutzer B stellt eine positive Testergebnismeldung (siehe "Covid-19-Testergebnismeldung") nach.</p> <p>Der App-Nutzer A prüft, ob seine App eine Warnung erhält.</p> <p>Dann startet App-Nutzer A die App erneut. Der App-Nutzer hat Zugriff auf einen "Einschalter" und kann diesen aktivieren.</p> <p>Der zweite App-Nutzer B startet seine App. Beide stellen den Kontaktfall (siehe unten "Kontaktfall") nach. Der App-Nutzer B stellt eine positive Testergebnismeldung (siehe "Covid-19-Testergebnismeldung") nach. Der App-Nutzer B prüft, ob seine App eine Warnung erhält.</p>	Vorlage Testprotokoll	
E03.01	Der App-Nutzer wird über die Konsequenzen des Ausschaltens informiert.	Ein App-Nutzer startet die App. Der App-Nutzer hat Zugriff auf einen "Ausschalter" und kann diesen aktivieren. Eine	Vorlage Testprotokoll	

E03.01	Der App-Nutzer wird über die Konsequenzen des Einschaltens informiert.	verständliche Meldung erscheint, die der Nutzer aktiv quittieren muss.	Vorlage Testprotokoll
E03.02	Der App-Nutzer kann die App über eine Einstellung in den Auslieferungszustand zurücksetzen. Inwiefern die gespeicherten Traces der letzten Tage erhalten bleiben; liegt außerhalb des Scope der App.	<p>Ein App-Nutzer startet die App und nimmt folgende Einstellungen in Schritt 1 vor:</p> <ul style="list-style-type: none"> • E01.02: Zustimmung zu den Nutzungsbedingungen und Datenschutzbedingungen erteilen • E01.03: Bestätigung zur Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe (Hash-Generierung) erteilen • E01.04: Bestätigung der Bluetooth-Nutzung (BLE) durch die Applikation erteilen • E01.05: Bestätigung zum Erhalt von Mitteilungen erteilen • E06.01 QR-Code zur Registrierung einscannen <p>Nutzung der App über 2 Tage (mindestens 2 pseudonyme IDs erzeugt) zur Erzeugung von lokalen Traces im Smartphone</p> <p>Der App-Nutzer setzt die App über die bereitgestellte Einstellung in den Auslieferungsstand zurück. Der App-Nutzer wiederholt alle Einstellungen aus Schritt 1. Im Backend wird für den neu eingescannten QR-Code ein positives Testergebnis hinterlegt. Der App Nutzer erteilt nach <u>E06.03 und E06.06 die</u></p>	Vorlage Testprotokoll

			<p>Zustimmung zur Übermittlung einer Warnung. Der App-Nutzer setzt die App über die bereitgestellte Einstellung in den Auslieferungsstand zurück.</p> <p>Validierung in der App:</p> <ul style="list-style-type: none"> • E01.02: Zustimmung zu den Nutzungsbedingungen und Datenschutzbedingungen ist erteilt • E01.03: Bestätigung zur Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe (Hash-Generierung) ist nicht erteilt • E01.04: Bestätigung zum Empfang von Mittellungen nicht erteilt • E06.01 Registrierung und QR-Code gelöscht • E06.03 und E06.06 Zustimmung zur Übermittlung einer Warnung nicht erteilt 	
E03.03	Ein Menü zu Applikationseinstellungen kann durch den App-Nutzer aufgerufen werden.	Ein App-Nutzer startet die App. Der App-Nutzer ruft das Menü für Applikationseinstellungen auf.	Vorlage Testprotokoll	
E03.03	Die Benachrichtigungen können ausgeschaltet werden.	Ein App-Nutzer startet die App. Der App-Nutzer ruft das Menü Applikationseinstellungen auf und schaltet Benachrichtigungen ein. "Das System" versendet eine Nachricht. Dieser Versand wird dem App-Nutzer nicht angezeigt (außer in der App nach Öffnen derselben).	Vorlage Testprotokoll	
E03.03	Der Nutzer kann über die Systemeinstellungen Bluetooth deaktivieren.	Ein App-Nutzer kann in den Systemeinstellungen Bluetooth deaktivieren, so dass das Contact Tracing funktionsunfähig ist.	Vorlage Testprotokoll	
E03.03	Die Zugriffsrechte der Applikation auf Bluetooth können ausgeschaltet werden.	Ein App-Nutzer A startet die App. Näherungsweise: Ein zweiter App-Nutzer B startet	Vorlage Testprotokoll	

			<p>seine App. Beide stellen den Kontaktfall nach (siehe unten "Kontaktfall"). Der App-Nutzer B stellt eine positive Testergebnismeldung (siehe "Covid-19-Testergebnismeldung) nach. Der App-Nutzer A prüft, ob seine App eine Warnung erhält. Er sollte dann keine erhalten.</p>	
E03.03		<p>Die Zugriffsrechte der Applikation auf Bluetooth können eingeschaltet werden.</p>	<p>Ein App-Nutzer A startet die App. Der App-Nutzer ruft das Menü Applikationseinstellungen auf und schaltet Bluetooth aus und stellt sicher, dass Bluetooth ausgeschaltet ist (siehe Prüffall dazu).</p> <p>Darauf hin schaltet er Bluetooth wieder ein. Ein zweiter App-Nutzer B startet seine App. Beide stellen den Kontaktfall (siehe unten "Kontaktfall") nach. Der App-Nutzer B stellt eine positive Testergebnismeldung (siehe "Covid-19-Testergebnismeldung) nach. Der App-Nutzer A prüft, ob seine App eine Warnung erhält. Er sollte eine Warnung erhalten.</p>	<p>Vorlage Testprotokoll</p>
E03.03		<p>Der App-Nutzer wird über die Konsequenzen des Ausschaltens informiert.</p>	<p>Ein App-Nutzer startet die App.</p> <ol style="list-style-type: none"> 1. Der App-Nutzer hat Zugriff auf die o.g. "Ausschalter" und kann diese aktivieren. 2. Eine verständliche Meldung erscheint, die der Nutzer aktiv quittieren muss. 	<p>Vorlage Testprotokoll</p>
E03.03		<p>Der App-Nutzer wird über die Konsequenzen des Einschaltens informiert.</p>	<p>Ein App-Nutzer startet die App.</p> <ol style="list-style-type: none"> 1. Der App-Nutzer hat Zugriff auf einen "Einschalter" und kann diesen aktivieren. 2. Eine verständliche Meldung erscheint, die der Nutzer aktiv quittieren muss. 	<p>Vorlage Testprotokoll</p>

[\(Link zur Prüffall-Matrix\)](#)

5.1.4 Kontaktfall (Begegnung mit infizierter Person)

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E04.01	Der App-Nutzer erhält eine Benachrichtigung in Form einer Notifikation, wenn er Kontakt zu einem infizierten App-Nutzer hatte.	<p>Vorbereitung:</p> <ol style="list-style-type: none"> 1. Das Testgerät wird in den Flugmodus versetzt 2. Eine pseudonymisierte ID aus dem Datenspeicher des Testgerätes wird auf dem Corona-Server hinterlegt und als infiziert gekennzeichnet. <p>Durchführung: Der App-Nutzer schaltet den Flugmodus aus. Das Gerät verbindet sich mit dem Internet und ruft die aktuellen Daten der identifizierten IDs vom Corona-Warn-App-Server ab. Das Gerät gleicht die aktuellen Daten mit dem internen Datenpool ab und erstellt eine Notifikation, welche dem App-Nutzer impliziert, dass ein Kontakt zu einer Person bestand, die sich als infiziert gemeldet hat.</p>	<p>Vorlage Testprotokoll</p>
	E04.01	Der App-Nutzer erhält eine Benachrichtigung in Form einer Notifikation, wenn sich das Risiko ändert.	<p>[Annahme: Die Risikoänderung (Statuswechsel) erfolgt über das CMS und wird zusätzlich oder mit der Abfrage nach den infizierten IDs von der App abgefragt.]</p> <p>Vorbereitung: Eine identifizierte pseudonymisierte Geräte-ID muss sowohl auf dem Corona-Warn-App-Server als auch im lokalen Datenspeicher der Applikation hinterlegt sein.</p> <p>Durchführung: Der CMS-Nutzer ändert das Risiko im Bezug auf die identifizierte pseudonymisierte Geräte-ID. Der App Nutzer</p>	<p>Vorlage Testprotokoll</p>

<p>E04.02</p>	<p>Der App-Nutzer kann über die Notifikation vom RKI hinterlegte Handlungsempfehlungen nachlesen.</p>	<p>erhält eine Notifikation mit einem Text, der die vorgenommene Änderung impliziert.</p> <p>Annahme: Die Handlungsempfehlungen sind statisch auf dem Gerät hinterlegt bzw. werden in regelmäßigen Abständen dort aktualisiert.</p> <p>Vorbereitung: siehe E04.01, Akzeptanzkriterium 1</p> <p>Durchführung: Der App-Nutzer öffnet die Notifikation durch einen Klick. Dort sieht er weitergehende Handlungsempfehlungen, die als scrollbarer Text in der Applikation angezeigt werden.</p>	<p>Vorlage Testprotokoll</p>
<p>E.04.03</p>	<p>Die Begegnungen werden nach 14 Tagen gelöscht.</p>	<p>Annahme: Die aus einer Begegnung resultierenden ID-Nummern müssen datenschutzkonform gelöscht werden.</p>	<p>Bestätigung von Apple und Google Das korrekte Löschen wird im Rahmen eines Langzeit-Usertests geprüft. Nach erfolgreichem GoLive wird dies überprüft.</p>
<p>Weitere abgeleitete Prüffälle zum Kontaktfall (Kennzeichnung: Exx.Ay)</p>			
<p>E04.A2</p>	<p>Bei positivem Testergebnis kann sich ein Mitarbeiter des Gesundheitsamts im CMS Daten zur Corona-App-Nutzung des Test-</p>	<p>Vorbereitung: Siehe E04.A1; App installieren</p> <p>Durchführung:</p>	<p>Nicht Bestandteil der Version 1.X und daher nicht abnahmerelevant.</p>

	<p>Kandidaten anzeigen lassen.</p>	<p>1. Mit passender Test-TeleTAN oder Test-QR-Code folgende Szenarien durchspielen:</p> <ul style="list-style-type: none">• Keine Registrierung von QR-Code oder TeleTAN passend zu positivem Test• Keine Push-Notifications bei Erhalt von Ergebnissen (sollte keine Auswirkung auf den Testfall haben) <p>Im CMS Portal-Server werden dem Mitarbeiter zu positiven Fällen angezeigt,</p> <ul style="list-style-type: none">- ob das Labor, welches den Test durchgeführt hat, den digitalen Prozess unterstützt,- ob das Testergebnis mit einer TeleTAN oder einem QR-Code verknüpft wurde,- ob der Proband die Corona-App installiert hat und- ob der Proband TeleTAN oder QR-Code zur Registrierung genutzt hat zum Erhalt von digitalen Testergebnissen. <p>Der Gesundheitsamts-Mitarbeiter nutzt diese Information zur Entscheidung, ob eine Kontaktaufnahme zum Nutzer mit Hilfe der Daten aus E04.A1 initiiert wird.</p> <p>Es sollte vorsorglich im Testprotokoll unter Verweis auf das Rollen- und Rechtskonzept vermerkt werden, dass technisch und organisatorisch ein Zugriff auf Daten nicht meldepflichtiger NutzerInnen durch den Mitarbeiter unmöglich ist.</p>	
--	------------------------------------	---	--

[Link zur Prüffall-Matrix](#)

5.1.5 Covid-19-Testergebnismeldung

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp Vorlage Testprotokoll
	E05.01	Positive Tests können eine Warnung auslösen.	<p>Schritte zum Auslösen einer Warnung siehe folgender Abschnitt 5.1.6 "<u>Auslösen einer Warnung</u>". Diese Schritte müssen durchlaufen werden.</p> <p>Der App-Nutzer soll beim Vorliegen eines positiven Testergebnisses dazu aufgefordert werden, IDs (pseudonymisiert) an den Warn-Server zu übermitteln.</p> <p>Nach dem er seine Zustimmung gegeben hat, sollten die IDs pseudonymisiert an den Warn-Server übermittelt werden.</p> <p>Im Warn-Server verifizieren, dass Daten an den Warn-Server übertragen wurden.</p>	<p>Inkl. Nachweis per Log-Auszug, dass Übermittlung erst nach Zustimmung erfolgt</p>
	E05.01	Positive Tests können keine weitere Warnung auslösen, wenn zuvor schon eine Warnung ausgelöst wurde.	<p><u>Vorbereitung:</u> Schritte zum Auslösen einer Warnung siehe folgender Abschnitt 5.1.6 "<u>Auslösen einer Warnung</u>". Diese Schritte müssen durchlaufen werden.</p> <p><u>Durchführung:</u></p> <p><u>Schritt 1:</u> Der App-Nutzer soll beim Vorliegen eines positiven Testergebnisses dazu aufgefordert werden, IDs (pseudonymisiert) an den Warn-Server zu übermitteln. Nachdem er seine Zustimmung gegeben hat, sollen die IDs pseudonymisiert an den Warn-Server zu übermittelt werden.</p> <p>Im Warn-Server soll verifiziert werden, dass Daten an den</p>	<p><u>Vorlage Testprotokoll</u></p> <p>Inkl. Nachweis per Log-Auszug für Schritte 1 und 2</p>

		<p>Warn-Server übertragen wurden.</p> <p>Schritt 2: Schritte zum Auslösen einer Warnung siehe "Auslösen einer Warnung" sollten ein weiteres Mal durchlaufen werden. Der App-Nutzer soll beim Vorliegen eines weiteren positiven Testergebnisses nicht erneut dazu aufgefordert werden, IDs (pseudonymisiert) an den Warn-Server zu übermitteln.</p> <p>Zur Sicherheit sollte im Warn-Server verifiziert werden, dass keine Daten an den Warn-Server übertragen wurden.</p>	
E05.01	Negative Tests können keine Warnung auslösen.	<p>Vorbereitung: Schritte zum Auslösen einer Warnung siehe folgender Abschnitt 5.1.6 "<u>Auslösen einer Warnung</u>". Diese Schritte müssen durchlaufen werden.</p> <p>Durchführung: Der App-Nutzer darf beim Vorliegen eines negativen Testergebnisses nicht dazu aufgefordert werden, IDs (pseudonymisiert) an den Warn-Server zu übermitteln.</p> <p>Zur Sicherheit sollte im Warn-Server verifiziert werden, dass im Falle eines negativen Testergebnisses keine Daten an den Warn-Server übertragen wurden.</p>	<p>Vorlage Testprotokoll, Nachweis per Log-Auszug,</p>
E05.01	Negative Tests ohne Resultat können keine Warnung auslösen.	<p>Vorbereitung: Schritte zum Auslösen einer Warnung siehe folgender Abschnitt 5.1.6 "<u>Auslösen einer Warnung</u>". Diese Schritte müssen durchlaufen werden.</p>	<p>Vorlage Testprotokoll inkl. Nachweis per Log-Auszug</p>

E05.02

**Benachrichtigung über den
Eingang des Testergebnisses**

Durchführung:
Der App-Nutzer darf ohne das Vorliegen eines Testergebnisses nicht dazu aufgefordert werden, IDs (pseudonymisiert) an den Warn-Server zu übermitteln. Zur Sicherheit sollte im Warn-Server verifiziert werden, dass im Falle eines fehlenden Testergebnisses keine Daten an den Warn-Server übertragen wurden.

Vorbereitung:
Schritte zum Auslösen einer Warnung siehe folgender Abschnitt 5.1.6 "Auslösen einer Warnung". Diese Schritte müssen durchlaufen werden.

Durchführung:
Der App-Nutzer soll beim Vorliegen eines positiven Testergebnisses dazu aufgefordert werden, IDs (pseudonymisiert) an den Warn-Server zu übermitteln. Nach dem er seine Zustimmung gegeben hat, sollte der App-Nutzer auf eine (Internet-) Seite weitergeleitet werden, die ihm weitere Informationen über die Erkrankung und nötige nächste Schritte bietet, um sein Verhalten an die Handlungsempfehlungen des RKI anpassen zu können.

Hierzu gehört die Anzeige eines Infotextes in der App mit definiertem Inhalt (z.B.: Informationen zum Ausgang des Testergebnisses, Informationen über erforderliche Maßnahmen, eine Hotline-Nummer etc.)

**Vorlage
Testprotokoll**

Weitere abgeleitete Prüffälle zur Testergebnismeldung (Kennzeichnung: Exx.Ay)

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E05.A1	Ein Test-Ergebnis kann digital in das Corona-Warn-App-Backend übertragen werden.	Dafür wird ein Testdatensatz (Dummy) als positiver Ergebnisdatsatz an das Backend übermittelt.	Vorlage Testprotokoll
	E05.A2	Einem Test-Vorgang wird ein QR-Code zugeordnet (GUID, "Globally Unique ID").	<p>Einer Probe bzw. Test-Anforderung wird ein QR-Code zugeordnet. Dieser Bezug bleibt durchgängig erhalten (E2E):</p> <ul style="list-style-type: none"> - Ausgabe durch Arzt/Test-Center - Scan durch Patienten - Registrierung - Annahme/Eingang Labor - Labor-Informationen-Server - Verifikations-Server - Notifikation. 	Vorlage Testprotokoll

[Link zur Prüfmatrix](#)

5.1.6 Auslösen einer Warnung

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E06.01	Ein auf dem Flyer des Arztes oder Test-Centers vorhandener QR-Code kann mit der Warn-App gescannt werden.	<p>Der App-Nutzer öffnet die Applikation und navigiert zum Menüpunkt für die Freischaltung des Abrufens von Test-ergebnissen via QR-Code. Die Applikation öffnet einen QR-Code-Scanner. Der QR-Code wird erfolgreich gescannt und der App-Nutzer erhält eine positive Bestätigung nach Einlesen des QR-Codes.</p> <p>Es ist möglich, einen eingelesenen QR-Code durch nochmaliges Einlesen eines anderen QR-Codes zu ersetzen, wenn der App-Nutzer z.B. aus</p>	Vorlage Testprotokoll

			<p>Vorsehen einen falschen QR-Code eingescannt hat, der nicht im Corona-Prozess genutzt wird.</p> <p>Alternative Variante:</p> <p>Dem Nutzer wird ein Hinweis eines nicht validen QR-Codes angezeigt. Da der QR-Code lediglich eine GUID beinhaltet, wird eine valide GUID über dessen Namensraum klassifiziert.</p>	
E06.01	Erklärungstext wird angezeigt.		<p>Der App-Nutzer führt die Schritte zum erfolgreichen Scan eines QR-Codes aus (siehe oben).</p> <p>Die App zeigt dem Benutzer einen Erklärungstext, in dem z.B. der weitere Prozess und der Umgang mit den Daten näher erläutert wird. Durch aktives Betätigen einer Bestätigung (z.B. "Ok-Button") verlässt der Benutzer den Erklärungstext.</p>	Vorlage Testprotokoll
E06.02	Der App-Nutzer erhält eine Benachrichtigung, sobald ein verifiziertes Testergebnis vorliegt.		<p>Vorbereitung:</p> <ol style="list-style-type: none"> 1. Der App-Nutzer führt einen erfolgreichen QR-Scan durch 2. Der mit dem QR-Inhalt verbundene Test wird mit einem verifizierten Testergebnis gekoppelt <p>Der App-Nutzer erhält eine Notifikation, sobald sich die Applikation mit dem Verifikations-Server verbunden und das Vorhandensein von Testergebnissen abgefragt hat.</p>	Vorlage Testprotokoll

<p>E06.02</p>	<p>Die Benachrichtigung enthält nicht das Ergebnis positiv oder negativ.</p>	<p>Der App-Nutzer führt die Schritte zum Erhalten einer Benachrichtigung bei einem Testergebnis durch.</p> <p>Auf dem Verifikations-Server wird für den QR-Code des App-Nutzers ein Testergebnis hinterlegt.</p> <p>Beim nächsten Abruf (Polling) zeigt das Smartphone eine Mitteilung an, die mitteilt, dass ein Test-Ergebnis vorliegt und dies in der Corona-App einsehbar ist mit Verweis auf die App. Das Ergebnis des Tests darf nicht bereits in der Push-Benachrichtigung stehen. Die Corona-App zeigt das Ergebnis des Tests mit Empfehlung nächster Schritte und Verhaltensweisen an.</p>	<p>Vorlage Testprotokoll,</p> <p>ggfs. in Kombination mit Screenshot</p>
<p>E06.03</p>	<p>IDs können pseudonymisiert an den Warn-Server übermittelt werden.</p>	<p>Prüfung von Datenpaketen, um sicherzustellen, dass nur die in E01.03 erstellte pseudonyme ID an den Warn-Server übermittelt wird und keine weiteren Daten, die den App-Benutzer als Person identifizierbar machen.</p>	<p>Vorlage Testprotokoll</p>
<p>E06.03</p>	<p>Übermittlung ist nur möglich, sofern zuvor eine Verifikation erfolgreich durchgeführt wurde</p>	<p>Ein Test, eine pseudonyme ID ohne eine vorhergehende Verifikation an den Warn-Server zu übermitteln, schlägt fehl.</p>	<p>Vorlage Testprotokoll</p>
<p>E06.03</p>	<p>Übermittlung ist nur möglich, sofern der App-Nutzer vorher zugestimmt hat.</p>	<p>Der App-Benutzer wird, nachdem er über das Vorliegen eines positiven Testergebnis benachrichtigt worden ist, gefragt, ob seine pseudonyme ID an den Warn-Server übermittelt werden darf.</p> <p>Der App-Benutzer erhält im Bestätigungsdialog alle notwendigen Informationen (z.B. etwaige Konsequenzen einer Bestätigung) und kann die Aktion bestätigen oder abbrechen.</p>	<p>Vorlage Testprotokoll</p>

		<p>Fall 1: Der App-Benutzer stimmt zu und die pseudonyme ID wird an den Warn-Server übergeben und ist in dessen Datenpool auffindbar.</p> <p>Fall 2: Die Übermittlung der ID wird unterbunden, weil der Benutzer die Zustimmung verweigert. Der Warn-Server erhält keine ID, diese ist nicht im Datenpool des Servers auffindbar.</p>	
E06.04	<p>Die zuständige Stelle (Gesundheitsamt oder Hotline) kann eine teleTAN generieren und diese dem App-Nutzer mitteilen. (generiert wird die teleTAN im Web-Interface des Portal-Servers, nicht durch das Call-Center selbst)</p>	<p>Als autorisierter Mitarbeiter (Gesundheitsamt oder Hotline) logge ich mich im Web-Interface des Portal-Servers ein und navigiere zum teleTAN-Generator und erstelle erfolgreich eine teleTAN.</p>	<p>Vorlage Testprotokoll</p>
E06.05	<p>Die Eingabe einer teleTAN innerhalb der App ist möglich.</p>	<p>Der App-Nutzer erhält eine teleTAN (erstellt durch einen Mitarbeiter des Gesundheitsamts in E06.04.).</p> <p>Der App-Nutzer öffnet die Applikation und navigiert zum Menüpunkt für die Freischaltung des Abrufens von Testergebnissen via TAN. Die Applikation öffnet einen Eingabedialog.</p>	<p>Vorlage Testprotokoll</p>
E06.05	<p>Überprüfung und Rückmeldung, ob die eingegebene teleTAN korrekt war (zu prüfen, ob technisch möglich).</p>	<p>Der App-Nutzer gibt die teleTAN erfolgreich ein und erhält eine positive Bestätigung nach Validierung und Prüfung des Inhalts.</p> <p>Variante: Eine TAN, die keinen validen Inhalt enthält, wird abgelehnt. Der Benutzer erhält eine Warnung.</p>	<p>Vorlage Testprotokoll</p>

E06.06	IDs können pseudonymisiert an den Warn-Server übermittelt werden.	siehe E06.03	Vorlage Testprotokoll
E06.06	Übermittlung ist nur möglich, wenn vorher eine Verifikation erfolgreich durchgeführt wurde.	siehe E06.03	Vorlage Testprotokoll
E06.06	Übermittlung ist nur möglich, sofern der App-Nutzer vorher zugestimmt hat.	siehe E06.03	Vorlage Testprotokoll

[Link zur Profil-Metrik](#)

5.1.7 Parametrisierung

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E07.01	Die Anpassung wird auf den Endgeräten vorgenommen, ohne dass ein Update der App erforderlich ist.	<p>Vorbereitung von Testdaten:</p> <p>Für jede Risiko-Wert-Kategorie erfolgt die Vorbereitung von identifizierten und nicht identifizierten pseudonymisierten IDs.</p> <p>Die identifizierten pseudonymisierten IDs sind dem Warn-Server zuvor bekannt gemacht worden und für den Austausch von Informationen zwischen mobiler Applikation und Server ist eine Freigabe des Benutzers erfüllt worden.</p> <p>Geprüft werden Kombinationen die sich aus den Schwellwerten und deren Auswirkung auf verschiedene App-Nutzer ergeben.</p> <p>Zum Beispiel: Ein RKI-Mitarbeiter erhöht einen Schwellwert mit Warnung in einer grafischen Oberfläche des Portal-Servers. Ein App-Nutzer, für den der Schwellwert relevant ist und der diesen zuvor nicht überschritten hatte, nun aber überschreitet, erhält eine Warnung.</p>	Vorlage Testprotokoll

[\(Link zur Prüffall-Matrix\)](#)

5.1.8 Technische Unterstützung

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E08.01	Telefonnummer der technischen Hotline ist in der Applikation hinterlegt.	Der App-Nutzer navigiert ins Hilfe-Menü und kann z.B. durch Anklicken der Hotline-Nummer einen Anruf starten. Der Anruf geht bei der offiziellen technischen Hotline der Applikation ein.	Vorlage Testprotokoll

[\(Link zur Prüffall-Matrix\)](#)

5.1.9 Barrierefreiheit

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E09.01	Die Barrierefreiheit bzgl. Sprachausgabe wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.	Prüfung von auf native mobile Apps anwendbaren Kriterien für Barrierefreiheit nach EN 301549 Chapter 11 für die jeweilige Zielplattform.	Vorlage eines Testats
	E09.02	Die Barrierefreiheit bzgl. Kontraste und Schrift wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.	Prüfung von auf native mobile Apps anwendbaren Kriterien für Barrierefreiheit nach EN 301549 Chapter 11 für die jeweilige Zielplattform.	Vorlage eines Testats

[\(Link zur Prüffall-Matrix\)](#)

5.1.10 Content Management

Prüf ID	# User Story ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	E10.01	Das Content-Management erfolgt auf Grundlage der Anforderungen des RKI	Zu prüfen ist, ob alle verwaltbaren gewünschten Inhalte in Form eines Content Management Systems (z.B. grafische Oberfläche auf dem Portalserver) so von RKI Mitarbeitern bearbeitet werden können, wie in einem gesonderten fachlichen Dokument des RKI gefordert.	Nicht Bestandteil der Version 1.X und daher nicht abnahmerelevant.
	E10.01	Der Content wird auf statische und dynamische Inhalte entsprechend der technischen Machbarkeit differenziert	Zu prüfen ist, ob alle als dynamisch vereinbarten Inhalte gemäß oben genannter Vorgehensweise ohne ein Update der Applikation aktualisierbar sind.	Nicht Bestandteil der Version 1.X und daher nicht abnahmerelevant.
	E10.01	Aktualisierungen der Parametrisierung erfolgen automatisch.	Zu prüfen ist, dass Aktualisierungen der Parametrisierung im Hintergrund gemeinsam mit dem automatischen Abgleich erfolgt.	Vorlage Testprotokoll

[Link zur Prüffall-Matrix!](#)

5.2 Prüffälle aus allgemeinen Qualitätskriterien

Um die mobile Applikation und das Gesamtsystem in einer hohen Qualität bereitzustellen und somit Akzeptanz und Erfolg zu fördern, müssen viele Aspekte beachtet werden. Dazu gehören zum Beispiel die Fragmentierung von mobilen Endgeräten auf dem Markt über viele Hersteller, Betriebssysteme und Betriebssystemversionen hinweg oder die hohen Anforderungen an die Benutzbarkeit ("Usability"). Es lohnt sich, diverse Werkzeuge zur automatisierten Qualitätsprüfung in den Entwicklungsprozess zu integrieren, um Kosten zu sparen und die Qualität fortwährend mit jeder neuen Funktionalität für die gesamte Applikation sicherzustellen. Aspekte wie Performanz, Zuverlässigkeit oder Sicherheit betreffen vor allem das Backend, welches auch bei einer hohen Anzahl von Infiltrierten Personen sicherstellt, dass Applikation stabil und funktional ist.

Folgende Qualitätskriterien der ISO25010 werden betrachtet:

- **Portabilität** (5.2.1)
- **Usability** (5.2.2)
- **Sicherheit** (5.2.3)
- **Performanz** (5.2.4)
- **Zuverlässigkeit** (5.2.5)
- **Funktionale Eignung** (5.2.6)

- **Kompatibilität** (5.2.7)
- **Wartbarkeit** (5.2.8)

ID	Prüfpunkt	Prüfvorgehen	Nachweise / Ergebnistyp
<p>5.2.1 Portabilität nach ISO25010 Kann die mobile Applikation auf einer Vielzahl von Endgeräten installiert und betrieben werden? Ist die Anwendung migrationsfest?</p>			
	Fragmentierung von Hardware für mobile Endgeräte ist betrachtet	Test der Bluetooth Funktionalität über parallele Verwendung von BT-Kopfhörern und App	Referenz der Gerätemodelle im Test sowie Testprotokoll
	Fragmentierung von Bildschirmgrößen und -auflösungen ist betrachtet	Test der Funktionalität (korrekte Darstellung) auf Geräten mit verschiedenen Auflösungen und Bildschirmgrößen.	Referenz der Gerätemodelle im Test und Auflistung von Auffälligkeiten
<p>5.2.2 Usability nach ISO25010 Sind die mobile Applikation und das CMS benutzerfreundlich und barrierefrei? (nicht enthalten: Betriebliche Administrations- und Management-Systeme)</p>			
	Das CMS ist barrierefrei.	Prüfung von Kriterien für Barrierefreiheit nach <ul style="list-style-type: none"> • BITV 2.0 . 	Nicht Bestandteil der Version 1.X und daher nicht abnahmerelevant.
	Die mobilen Applikationen sind (soweit wie für die Plattformen möglich) barrierefrei.	Prüfung von Kriterien für Barrierefreiheit nach <ul style="list-style-type: none"> • EN 301549 Chapter 11 in Anwendbarkeit auf native mobile Apps. 	Vorlage eines Testats
	Die mobile Applikation ist für alle identifizierten Nutzergruppen benutzbar	Prüfung der vereinbarten Kriterien für Usability und User Experience und Qualitätsrichtlinien von Google und Apple (siehe oben).	Ergebnisprotokolle von Fokusgruppen und UX-Tests
	Das CMS ist für das Pflegen von	Prüfung von Kriterien für Usability und User Experience nach <ul style="list-style-type: none"> • ISO 9241-210 	Nicht Bestandteil der Version 1.X und nicht Bestandteil des

Inhalten nutzbar	<ul style="list-style-type: none"> • ISO 9241-110 • ISO 9241-112 	Leistungsumfangs und daher nicht abnahmerelevant.
5.2.3 Sicherheit nach ISO25010 Ist die Anwendung sicher und entspricht den Vorgaben des Datenschutzes?		
Anwendung implementiert Vorkehrungen, um die Sicherheitskriterien zu erfüllen	Zu betrachtende Sicherheitskriterien: <ul style="list-style-type: none"> • Integrität • Vertraulichkeit • Authentizität • Zurechenbarkeit • Verbindlichkeit 	Vorlage Sicherheitskonzepte der Dienstleister gemäß Anlage 4
Die Anwendung fordert nur die minimale Teilmenge von Berechtigungen. Diese werden erst gefordert, wenn der Benutzer Gebrauch der entsprechen den Funktionalität macht.	Die Anwendung folgt jederzeit einem klaren, datenschutz-konformen Konzept.	Vorlage Konzepte für Datenschutz, Sicherheit, Rollen und Rechte gemäß Anlage 4
5.2.4 Performanz nach ISO25010 Sind Zeitverhalten, Ressourcenverbrauch und Kapazität angemessen?		
Die mobile Applikation reagiert im normalen Betrieb angemessen schnell	Test von: <ul style="list-style-type: none"> • Installation • Erster Applikationsaufruf • Weitere Applikationsaufrufe • Große Datensätze • Verwendung von Bluetooth-Hardware • Grafische Benutzeroberfläche 	Vorlage einer Referenz getesteter Gerätemodelle, aus der evtl. Auffälligkeiten hervorgehen (dafür spezifische Testfälle sind nicht erforderlich)
Die Kapazitäten reichen auch	Test von: <ul style="list-style-type: none"> • sehr große Anzahl zeitgleicher Sessions • sehr große Anzahl an Erkrankten 	Vorlage Testprotokoll

für große Benutzerzahlen aus	•	
Der Verbrauch von Ressourcen ist angemessen	Betrachtung von: <ul style="list-style-type: none"> • Energieverbrauch • Arbeitsspeicher • Applikationsgröße 	Technische Kennzahlen der Applikation basierend auf den von Apple/Google zur Verfügung gestellten Informationen
5.2.5 Zuverlässigkeit nach ISO25010 Sind mobile Applikation und Backend verfügbar und reagieren im Fehlerfall angemessen?		
Wechsel zwischen Hoch- und Querformat erfolgt fehlerfrei	Test des Wechsels in einzelnen Testscreens auf verschiedenen Endgeräten	Vorlage Testprotokoll
Unterbrechungen (z.B. Anrufe, manuelles Abschalten) führen zu keinen Fehlerfällen oder Datenverlust	Test von <ul style="list-style-type: none"> • eingehenden Anrufen • manuellem Abschalten • Ladekabel anschließen • Entfernen der Batterie während laufender Nutzung. 	Vorlage Testprotokoll
Statusübergänge (z.B. App wird in den Hintergrund geschickt) führen zu keinen Fehlerfällen oder Datenverlust	Test von: <ul style="list-style-type: none"> • Applikation in den Hintergrund schicken • Durch Notifikation in andere Applikationen wechseln während laufender Nutzung. 	Vorlage Testprotokoll
Applikation funktioniert auch bei Netzwerkproblemen / offline (z.B. statische Inhalte werden angezeigt,	Test von: <ul style="list-style-type: none"> • Oberfläche und Inhalt im Offline-Modus • Notwendige Service-Aufrufe bei geringer Netzwerkverbindung während laufender Nutzung. 	Vorlage Testprotokoll

<p>Internet- verbindung nur für notwendige Interaktionen notwendig)</p>		
<p>Fehler und Abstürze können verfolgt und analysiert werden</p>	<p>Vorgehen zur Prüfung der Implementierung von Bug-Reports und Logging:</p> <ul style="list-style-type: none"> • Fehler oder Absturz in der App provozieren z.B. durch Manipulation des Host Betriebssystems (Speicher voll etc.) • Dem Nutzer wird direkt nach Fehlereintritt oder bei Absturz nach Restart der App eine sprechende Fehlermeldung angezeigt mit hoher Selbstbeschreibungsfähigkeit (vgl. ISO 9241-112) und Hinweis auf die technische Hotline • Der Nutzer kann diesen Hinweis schließen und ignorieren oder weitere Aktivitäten vornehmen, vgl. Alternative 1 oder 2. In der Umsetzung ist Alternative 1 zu priorisieren, nur wenn diese Alternative technisch unzureichend oder die erforderliche manuelle Übermittlung unzumutbar ist, ist Alternative 2 in Betracht zu ziehen. <p>Alternative 1:</p> <ul style="list-style-type: none"> • Der App-Nutzer ruft freiwillig bei der technischen Hotline an und gibt telefonisch die Bug-Report Daten an, die in der App zum Fehler dargestellt werden • Der Hotline übernimmt die Bug-Report-Daten manuell in ein passendes Bugtracking-System • Es findet explizit keine automatische Datenübertragung zwischen App und Backend bzgl. Fehlerreporting statt • Der durch die technische Hotline erfasste Bug-Report bietet ausreichend Details, so dass ein am Testaufbau nicht beteiligter 	<p>Nicht für Version 1.X relevant und nicht Bestandteil des Leistungsumfange und daher nicht abnahmerelevant</p>

	<p>Entwickler den Fehler reproduzieren und diesen abstellen kann</p> <p>Alternative 2:</p> <ul style="list-style-type: none"> • Der App-Nutzer wird unaufdringlich um Erlaubnis gebeten einen anonymisierten Bug-Report an das Backend abzuschicken, der Nutzer wird dabei vollumfänglich über den Zweck dieser Daten und den Umfang der bei Zustimmung übermittelten Daten informiert • Die App generiert bei Zustimmung einen Bug-Report mit den gleichen Ansprüchen an die Datenübertragung und Dateninhalt bzgl. Anonymisierung wie die Übertragung einer Warnung mit Übermittlung der pseudonymen IDs • Die App löscht den Bug-Report nach Versand sicher • Die Zustimmung zum Versand von Bug-Reports wird nicht gespeichert und wird mit jedem weiteren Vorkommen eines schweren Fehlers durch den App-Nutzer erneut abgefragt • Der Bug-Report bietet ausreichend Details, so dass ein am Testaufbau nicht beteiligter Entwickler den Fehler reproduzieren und diesen abstellen kann 	
<p>Der Absturz einer Serverkomponente führt zu keiner Downtime des gesamten Backends</p>	<p>Test der Applikation, wenn einzelne Serverkomponenten heruntergefahren sind. Zum Beispiel: Ist das Erstellen einer TAN möglich, wenn der Corona-Warn-App-Server heruntergefahren ist?</p>	<p>Vorlage Testprotokoll</p>
<p>Das Backend lässt sich nach einem Fehlerfall oder Absturz in</p>	<p>Betrachtung von:</p> <ul style="list-style-type: none"> • Applikationsgröße • Einträge in Datenbank • Datenspeicher 	<p>Vorlage Testprotokoll, Technische Kennzahlen</p>

	angemessen er Zeit ohne Datenverlust hochfahren.		
5.2.6 Funktionale Eignung nach ISO25010 Ist die gewünschte Funktionalität für die mobile Applikation und das Backend korrekt implementiert?			
Die mobile Applikation funktioniert, wie in den User Stories beschrieben	Es ist ein Testkonzept vorhanden, das <ul style="list-style-type: none"> • funktionale Tests • Regressionstests • API-Tests für Backend und Frontend durchführt.	High-Level-Testplan	
Alle fachlichen Anforderungen werden getestet.	Jedes Akzeptanzkriterium wird durch mindestens einen funktionalen Test sichergestellt.	Testspezifikation / Beleg Testabdeckung für fachliche Funktionalität	
5.2.7 Kompatibilität nach ISO25010 Ist ein fehlerfreier Datenaustausch zwischen allen beteiligten Systemen gegeben?			
Der Datenaustausch mit dem Backend funktioniert für alle betroffenen Betriebssysteme fehlerfrei	Test aller Schnittstellen und Serviceaufrufe für die Betriebssysteme: <ul style="list-style-type: none"> • Android • IOS 	Testprotokolle für Integrations- und Contact-Testing	
Datenobjekte und Frameworks der unterschiedlichen Betriebssysteme sind kompatibel	Überprüfen des Konzepts auf mögliche Datenmissstände, wie z.B. durch doppeltes Erstellen einer pseudonymen ID von unterschiedlichen Geräten oder Inkonsistenzen unterschiedlicher Libraries und Frameworks auf IOS und Android.	Schnittstellen-spezifikation / Kontrakte	
5.2.8 Wartbarkeit nach ISO25010 Sind die Komponenten/Module/Software leicht zu ändern, erweitern, testen, verstehen?			

<p>Die Mobile Applikation und das Backend können schnell an Marktbedingungen angepasst werden (z.B. Bugfixes, neue Funktionalität) und haben eine geringe Time-To-Market.</p>	<ul style="list-style-type: none"> Integration und Deployment sind über eine Continuous Delivery Pipeline für alle relevanten Backend-Komponenten standardisiert und automatisiert. Ein „Release on Demand“ ist für alle relevanten Backend-Komponenten möglich (vgl. https://www.scaledagileframework.com/release-on-demand/) 	<p>ISO 9001 Zertifikat</p>
<p>Die Mobile Applikation ist modular aufgebaut.</p>	<p>Die zugrundeliegende Softwarearchitektur beachtet</p> <ul style="list-style-type: none"> IOS Best Practices empfohlen von Apple (vgl. https://developer.apple.com/documentation) Android Best Practices empfohlen von Google vgl. (https://developer.android.com/learn/develop/ui-components) 	<p>https://github.com/corona-warn-app/cwa-architecture/blob/master/solution_architecture.md</p>
<p>Das Backend ist modular aufgebaut.</p>	<p>Die zugrundeliegende Softwarearchitektur beachtet Konzepte der Modularität:</p> <ul style="list-style-type: none"> Schnitt in Microservices Trennung von Presentation, Business und Data Access Layer Verwendung von Design-Patterns wie MVC oder MVP Validierung der Architektur über z.B. Sonargraph-Architect (wenn Backend in C#, C/C++ oder Java implementiert) ansonsten entsprechendes anderes Tool (es darf keine Zyklen oder Abweichungen von der Schichtenarchitektur geben) 	<p>https://github.com/corona-warn-app/cwa-server/blob/master/docs/architecture-overview.md</p>
<p>Schnittstellen sind dokumentiert und einheitlich implementiert.</p>	<p>Schnittstellen sind formal-definiert, folgen den OpenAPI Spezifikation Best Practices (https://www.openapis.org/) und sind über ein geeignetes Tool implementiert / beschrieben (z.B: Swagger, vgl. https://swagger.io/)</p>	<p>Schnittstellen-Spezifikation gemäß Anlage 1</p>
<p>Der Source-Code wird unter der</p>	<ul style="list-style-type: none"> Entwicklungsprojekt verwendet automatische Code- 	<p>Nicht abnahmerelevant, aber nachzureichen: Werkzeugreport,</p>

Anwendung von Qualitätsmerkmalen für wartbaren Code geschrieben.	Qualitätsprüfungs- Tools (z.B.: Sonarqube o.ä.). <ul style="list-style-type: none"> • Coding-Guidelines sind etabliert und angewendet • Das Projekt verwendet automatisierte Code-Formatierung und eine gemeinsame Normenkatur 	Coding-Guidelines
--	--	-------------------

5.3 Prüffälle: Anforderungen aus App-Plattform Guidelines

Für die Zielplattformen Android und iOS gibt es von Google und Apple diverse relevante Guidelines. Das wird dadurch nachgewiesen, dass die App in den Stores angenommen wurde:

Damit die jeweiligen Apps für die Plattform Nutzer gut benutzbar sind, sollen diese den UX Konventionen der Plattform Anbieter - unter Berücksichtigung der Corporate Identity Vorgaben des RKI oder des Bundes entsprechen.

UX-Standards

Die Einhaltung der UX-Standards ist in Kapitel 5.2 adressiert (Prüffälle der allgemeinen Qualitätskriterien).

- Apple: <https://developer.apple.com/design/human-interface-guidelines/ios/overview/themes/>
- Google: <https://material.io/design/guidelines-overview>

Anforderungen an den Entwicklungsprozess

Ebenso stellen beide Anbieter technische Guidelines zur plattform-spezifischen Entwicklung von mobilen Applikationen bereit.

Die Einhaltung der Hersteller-Anforderungen an den technischen Entwicklungsprozess sind in Kapitel 5.2 aufgeführt (Prüffälle: Anforderungen an den Entwicklungsprozess).

- Apple: <https://developer.apple.com/app-store/resources/>
- Google: <https://developer.android.com/guide>

App Store

Jede Anwendung, die in Google Play oder den AppStore angeboten wird, durchläuft einen mehrstufigen Prozess, mit dem sichergestellt wird, dass die App den Richtlinien der Store-Betreiber entsprechen.

Diese sind:

- Apple: <https://developer.apple.com/app-store/review/guidelines/>
- Google: <https://play.google.com/about/developer-content-policy/>

Um sicherzustellen, dass die App nicht abgelehnt wird, ist sicherzustellen:

ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	<ul style="list-style-type: none"> • Compliance von Design und Code 		Nachweis, dass App im Store akzeptiert wurde
	<ul style="list-style-type: none"> • Eintragung im Store (Artefakte) 		Nachweis, dass App im Store akzeptiert wurde
	<ul style="list-style-type: none"> • App APK und IPA sind geprüft gegen automatische pre-deploy Werkzeuge von Apple und Google und alle signalisierten Probleme aufgelöst 		Nachweis, dass App im Store akzeptiert wurde

5.2 Prüffälle aus Anforderungen der Informationssicherheit und des Datenschutzes

Die Corona-Warn-App und das Backend-System verarbeiten sensible und besonders schützenswerte persönliche Daten und müssen daher den in den Projektverträgen festgelegten Informationssicherheits- und Datenschutzstandards entsprechen.

Daraus ergeben sich die folgenden Prüfpunkte:

ID	Prüfpunkt	Prüfvorgehen	Nachweis / Ergebnistyp
	Berücksichtigung der Anforderungen an die Informationssicherheit	Die Entwickler und Tester kennen und berücksichtigen die Anforderungen an die Informationssicherheit.	Sicherheitskonzepte gemäß Anlage 4
	Berücksichtigung der Anforderungen an den Datenschutz	Die Entwickler und Tester kennen und berücksichtigen die Anforderungen an den Datenschutz.	Datenschutzkonzepte gemäß Anlage 4

**Weitere Prüffälle und mögliche Nachweise zum Datenschutz sind enthalten in:
 Prüffälle aus allgemeinen Qualitätskriterien (Abschnitt 5.2.3 Sicherheit nach ISO25010).**

5.3 Prüffälle aus Anforderungen der Barrierefreiheit

Die mobilen Anwendungen (Apps) sowie die User Interfaces außerhalb der App entsprechen dem vereinbarten Umfang nach EN 301549 konform (bezogen auf die App nach EN 301 549 Chapter 11 in Anwendbarkeit auf native mobile Apps).

Zur Barrierefreiheit sind Prüffälle und mögliche Nachweise enthalten in:

- Prüffälle aus User Stories (Abschnitt 5.1.9 Barrierefreiheit) sowie
- Prüffälle aus allgemeinen Qualitätskriterien (Abschnitt 5.2.2 Usability).

6. Ergebnisdokumentation

In Abgrenzung zu diesem Leitfaden sind zur Dokumentation der Prüfergebnisse vorzulegen:

- Test-Konzept (z.B. Word, Übergabe PDF/A)

(z.B. Word → Übergabe-Format: PDF/A)

- Test-Protokoll (z.B. Excel oder Tool-Export, Übergabe PDF/A)

(Excel oder Tool-Export → Übergabe-Format: PDF/A)

- Test-Bericht (z.B. Word, Übergabe PDF/A)

(Word , vorzugsweise auf Grundlage V-Modell XT Bund/ITZBund → Übergabe-Format: PDF/A)

- Ergebnis-Präsentation (z.B. PowerPoint, Übergabe PDF/A)

(*Management Summary / Entscheider-Präsentation in Powerpoint o.ä. Aufbereitung → Übergabe-Format: PDF/A*).

Glossar

Folgende Abbildung gibt eine Übersicht über die geplante Systemlandschaft der Corona-Warn-App (Stand 27.05.2020):

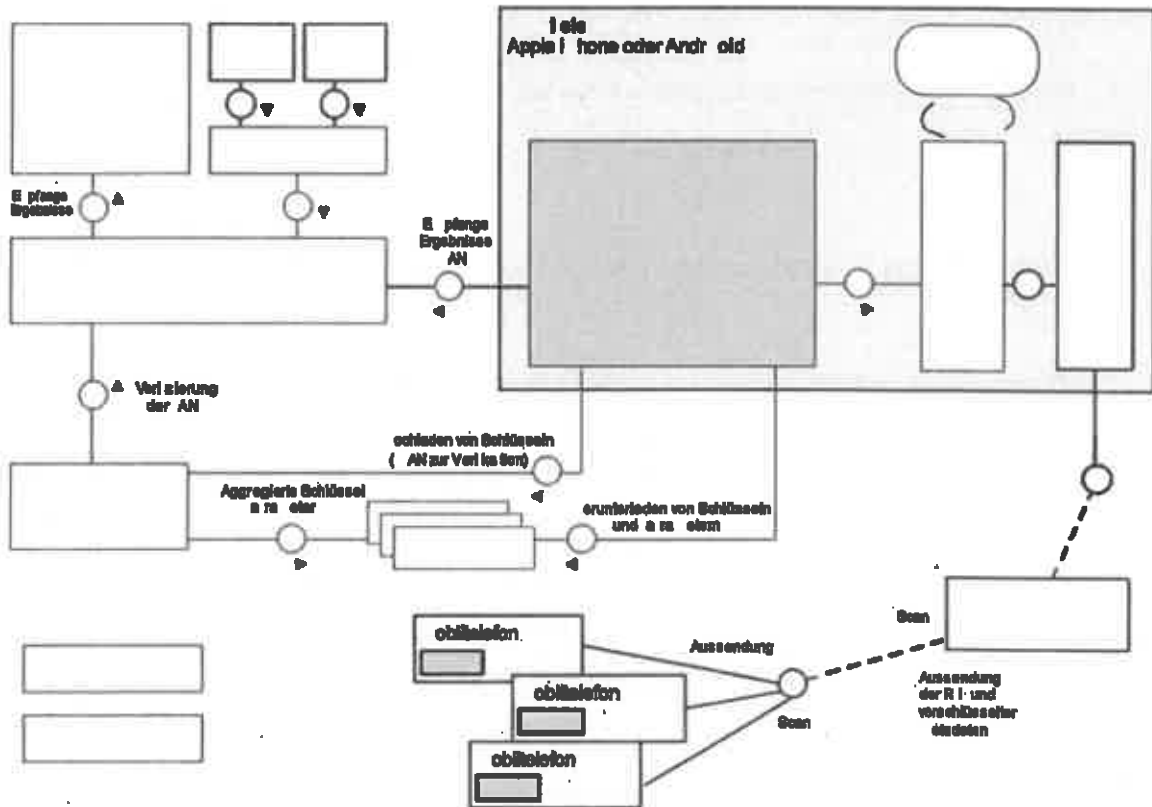


Abbildung 5: Übersicht Systemlandschaft Corona-Warn-App

Einzelne in diesem Dokument referenzierte Systemkomponenten sind zur Erläuterung des Gesamtprozesses in der folgenden Tabelle stichpunktartig beschrieben (auf Grundlage der Veröffentlichung im GitHub, Stand 27.05.2020):

Systemkomponente	Erläuterung
Corona-Warn-App (CWA)	Mit der Corona-Warn-App (CWA) können Einzelpersonen ihr persönliches Expositionsrisiko mithilfe ihrer Mobiltelefone verfolgen und Testergebnisse abrufen.
Portal-Server	Der Portal-Server dient mehreren Nutzergruppen (wo er in den User Stories erwähnt wird) mit unterschiedlicher Funktionalität:

	<p><u>Hotline Mitarbeiter:</u></p> <ul style="list-style-type: none"> • Workflow-gestützte Auskunft zu technischen, datenschutzbezogenen, gesundheitsbezogenen, psychologischen und Fragen zum Prozess der Verifikation von Test- Ergebnissen. • Generierung einer teleTAN <p><u>RKI:</u></p> <ul style="list-style-type: none"> • Konfiguration von Schwellwerten für die Risikobewertung, orientiert an Vorhersagen zu Auswirkungen bei Änderungen • Content-Management von Texten in der Corona-Warn-App <p><u>Gesundheitsämter:</u></p> <ul style="list-style-type: none"> • Generierung einer Tele-TAN • Bei positivem Testergebnis Anzeige zur Corona-App-Nutzung des Test-Kandidaten, um über telefonische Benachrichtigung entscheiden zu können
Verifikations-Server	<p>Der Verifikations-Server wird querschnittlich von diversen Komponenten genutzt. Er leistet die Verifikation von mit QR-Codes und TAN-Nummern verknüpften Daten, um Manipulationen auszuschließen (s. Abbildung 5: Übersicht Systemlandschaft Corona-Warn-App).</p>
Corona-Warn-App-Server	<p>Der Corona-Warn-App Server nimmt im Warnungsfall von Corona-Warn-App-Nutzern pseudonyme Schlüssel mit Verifizierungs-TAN entgegen und stellt Corona-Warn-App-Nutzern durch Gesundheitsbehörden aktualisierte Parameter zur lokalen Konfiguration bereit, sowie im aktuellen Zeitfenster relevante pseudonyme Schlüssel anderer Nutzer, die Ihre Infizierung freiwillig gemeldet haben zur lokalen Kontaktfall-Identifizierung.</p>
Exposure Notification Framework	<p>Neues Framework für dezentrale Kontaktverfolgung, entwickelt durch Apple und Google (vgl. https://www.apple.com/covid19/contacttracing)</p>
Labor-Informationssystem (LIS)	<p>Nimmt von Laboren Testergebnisse mit QR-Code entgegen. Bei positivem Testergebnis bekommt der Mitarbeiter des Gesundheitsamts gem. §9 IfSG persönliche Daten zum Test-Kandidaten im LIS durch das Labor übermittelt.</p>

Abbildung 6: Kurzbeschreibung Systemkomponenten

Abbildungsverzeichnis

Abbildung 1: Qualitäts-Dimensionen des ISO-Standards 25010	8
Abbildung 2: Tabelle der Fehler-Kategorien	10
Abbildung 3: Tabellarisches Prüfschema	12
Abbildung 4: Matrix der Prüffälle aus den User Stories	16
Abbildung 5: Übersicht Systemlandschaft Corona-Warn-App	49
Abbildung 6: Kurzbeschreibung Systemkomponenten	50

Anhang

Übersicht der User Stories (Stand 14.05.2020)

Hier finden Sie eine Übersicht der User Stories mit Stand 14.05.2020, welche als Grundlage für Kapitel 5.1 Prüffälle der User Stories dienen.

Die Anforderungen an die Corona-Warn-App, die den fachlichen Umfang der Anwendung definieren, wurden in der üblichen Form aus Nutzersicht formuliert:

„Als <Stakeholder> möchte ich <Handlung durchführen>, um <gewünschtes Ergebnis zu erzielen>.“

Die zugehörigen Akzeptanzkriterien der User Stories ergänzen die Spezifikation der Anforderungen; indem sie Bedingungen definieren, welche die Software erfüllen muss, um die Bedürfnisse der Kunden zu befriedigen.

Anbahnung und Installation (Onboarding-Prozess)

# User Story ID	User Story	Akzeptanzkriterien
E01.01	Als App-Nutzer möchte ich beim erstmaligen Start der Applikation eine Einleitung zur Funktionsweise der Applikation erhalten (App-Motivation).	<ol style="list-style-type: none"> 1. Einführung in die Funktionsweise der App wird bei erstmaligem Start der Applikation <u>angezeigt</u>. 2. Einführung in die Funktionsweise der App wird bei weiteren Startvorgängen <u>nicht angezeigt</u>. 3. Die erklärenden Inhalte sind in den jeweiligen Funktionsbereichen für den App-Nutzer vorhanden.
E01.02	Als App-Nutzer möchte ich beim erstmaligem Applikationsstart über die Nutzungsbedingungen und Datenschutzbestimmungen (Data Protection Screen) informiert werden und meine Zustimmung geben, um über den Umgang mit meinen Daten innerhalb der Anwendung aufgeklärt zu sein.	<ol style="list-style-type: none"> 1. Mit Nutzung der App akzeptiert der App-Nutzer die Nutzungsbedingungen und <u>Datenschutzbestimmungen</u>. 2. Die Nutzungsbedingungen sind innerhalb der App einsehbar. 3 Die Abfrage erfolgt nur bei der erstmaligen Nutzung.
E01.03	Als App-Nutzer möchte ich bei erstmaliger Nutzung der Applikation gefragt werden, ob ich der Erstellung pseudonymer IDs und deren Aussendung an Geräte in meiner Nähe durch die App zustimme, damit ich über die Funktionsweise der Applikation informiert bin.	<ol style="list-style-type: none"> 1. Eine Bestätigung der Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe durch die Applikation ist <u>Voraussetzung für die App-Nutzung</u>. 2. Nach der erstmaligen Nutzung erfolgt die <u>Abfrage nicht</u>.
E01.04	Als App-Nutzer möchte ich bei erstmaliger Nutzung der Applikation gefragt werden, ob die Applikation auf die Bluetooth-Funktion des Smartphones zugreifen darf, damit ich die mobiltelefonseitige Nutzung der Applikation kontrollieren kann.	<ol style="list-style-type: none"> 1. Eine Bestätigung der Bluetooth-Nutzung (BLE) erfolgt durch die Nutzung der Applikation.
E01.05	Als App-Nutzer möchte ich bei erstmaliger Nutzung der Applikation gefragt werden, ob die Applikation mir Benachrichtigungen schicken darf,	<ol style="list-style-type: none"> 1. Eine Abfrage zu den <u>Benachrichtigungseinstellungen</u> der Applikation findet vor erstmaliger Nutzung <u>statt</u>.

E01.06	damit in verschiedenen Situationen Push-Notifications ausgespielt werden können. Als App-Nutzer möchte ich bei erstmaliger Nutzung der Applikation meine Sprache angezeigt bekommen, damit die Nutzung der App für mich verständlich ist.	2. Nach der erstmaligen Nutzung erfolgt die Abfrage nicht. 1. Erkennung der eingestellten System Sprache wird durchgeführt. 2. Wenn die erkannte System Sprache nicht im Content hinterlegt ist, wird im Default Englisch ausgewählt. 3. In der ersten Version der App ist Mehrsprachigkeit vorgesehen.
E01.07	Als App-Nutzer möchte ich bereits während des Onboardings Hilfen und Einstellungen zur Barrierefreiheit bekommen, um die App nutzen zu können.	1. Die Barrierefreiheit wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.

Informationen und Instruktionen zur Nutzung der Applikation

# User Story ID	User Story	Akzeptanzkriterien
E02.01	Als App-Nutzer möchte ich Zugriff auf eine FAQ-Liste haben, um mir bei Fragen zur Applikation selbst weiterhelfen zu können.	1. Ein Link auf eine Internetseite mit FAQs ist im Applikationsmenü hinterlegt.
E02.02	Als App-Nutzer möchte ich Zugriff auf eine Anleitung zur Applikation haben, um die Anwendung und ihre Funktionen zu verstehen.	1. Ein Link auf eine Internetseite mit Benutzerhandbuch ist im Applikationsmenü hinterlegt.
E02.03	Als App-Nutzer möchte ich Zugriff auf ein Erklärvideo zur Applikation haben, um die Anwendung und ihre Funktionen zu verstehen.	1. Ein Link auf eine Internetseite mit Erklärvideo ist im Applikationsmenü hinterlegt.
E02.04	Als App-Nutzer möchte ich das Impressum der Applikation einsehen können, um zu sehen, wer für Entwicklung und Inhalte der Applikation verantwortlich ist.	1. Es gibt ein Untermenü "Impressum". 2. Das Impressum beinhaltet die üblichen Angaben zur Impressumspflicht.
E02.05	Als App-Nutzer möchte ich Nutzungsbedingungen und Datenschutzinformation jederzeit einsehen können.	1. App bietet einfachen Zugriff auf Nutzungsbedingungen und Datenschutzinformation
E02.06	Als App-Nutzer möchte ich die verschiedenen Hotlines zu technischen, datenschutzbezogenen, gesundheitsbezogenen und psychologischen Fragestellungen sowie zur Verifikation eines Testergebnisses angezeigt bekommen, damit ich weitere Informationen erhalte oder Fragen beantwortet bekomme.	1. Anzeige der Telefonnummern der Hotlines (für technische, datenschutzbezogene, gesundheitsbezogene und psychologische Fragestellungen) 2. Anzeige der zeitlichen Erreichbarkeit der Hotlines (z.B.: 24/7) 3. Telefonnummern können direkt aus der App gewählt werden.

Nutzung im Regelprozess

# User Story ID	User Story	Akzeptanzkriterien
E03.01	Als App-Nutzer möchte ich die Applikation aktivieren und deaktivieren können, um die Funktion ein- und auszuschalten.	1. Eine Umschaltfläche schaltet die Funktion (Bluetooth im Hintergrund und Hashgenerierung) ein und aus. 2. Die Konsequenzen des Ein-/Ausschaltens werden erklärt.

E03.02	Als App-Nutzer möchte ich die App in den "Delivery Default" zurücksetzen können, damit ich sie neu konfigurieren kann.	1. Die App kann über eine Einstellung in den Auslieferungszustand zurückgesetzt werden, die gespeicherten Traces der letzten Tage bleiben aber erhalten.
E03.03	Als App-Nutzer möchte ich die Applikationseinstellungen (Zugriffrechte, z.B. Bluetooth, Benachrichtigungen) in einem Menü anpassen können, um Funktion und Zugriffe der Applikation verwalten zu können.	<p>1. Ein Menü zu Applikationseinstellungen kann durch den App-Nutzer aufgerufen werden.</p> <p>2. Die Benachrichtigungen können ein- und ausgeschaltet werden.</p> <p>3. Die Zugriffsrechte der Applikation auf Bluetooth können durch den App-Nutzer erteilt und entzogen werden.</p> <p>4. Vor Deaktivierung der Zugriffsrechte erhalte ich Informationen darüber, welche Funktionen der App dadurch nicht mehr (vollumfänglich) funktionieren</p>

Kontaktfall (Begegnung mit Infizierter Person)

# User Story ID	User Story	Akzeptanzkriterien
E04.01	Als App-Nutzer möchte ich informiert werden, wenn eine Person, zu der ich Kontakt hatte, sich als infiziert gemeldet hat. Damit kann ich geeignete Maßnahmen treffen, um die Verbreitung des Virus zu stoppen.	<p>1. Eine Notifikation durch die Applikation wird an den App-Nutzer verschickt.</p> <p>2. Die Notifikation informiert den App-Nutzer über eine Risikoänderung (in Abhängigkeit der zur Verfügung gestellten API-Funktion)</p>
E04.02	Als App-Nutzer möchte ich im Kontaktfall Handlungsanweisungen durch die Applikation bekommen, um mein Verhalten an die Empfehlungen des RKI anzupassen.	1. Die Notifikation führt zu hinterlegten Handlungsempfehlungen für den Kontaktfall.

Covid-19-Testergebnismeldung

# User Story ID	User Story	Akzeptanzkriterien
E05.01	Als RKI möchte ich, dass ausschließlich positiv getestete Nutzer einmalig eine Warnung auslösen können, um Missbrauch zu vermeiden.	<p>1. Nur positive Tests können eine Warnung auslösen.</p> <p>2. Für jeden Test kann nur einmal eine Warnung ausgelöst werden.</p>
E05.02	Als App-Nutzer möchte ich im Falle eines positiven Testergebnisses Informationen über die Erkrankung und nötige nächste Schritte bekommen, um mein Verhalten an die Handlungsempfehlungen des RKI anpassen zu können.	<p>1. Benachrichtigung über den Eingang des Testergebnisses</p> <p>2. Anzeige eines Infotextes in der App mit definiertem Inhalt (z.B.: Informationen zum Ausgang des Testergebnisses, Informationen über erforderliche Maßnahmen, eine Hotline-Nummer)</p>

Auslösen einer Warnung

# User Story ID	User Story	Akzeptanzkriterien
E06.01	Als App-Nutzer möchte ich einen von meinem Arzt oder Test-Center ausgehändigten QR-Code scannen können, damit mir später das Testergebnis in der Warn-App zur Verfügung gestellt werden kann.	<p>1. Ein auf dem Flyer des Arztes oder Test-Centers vorhandener QR-Code kann mit der Warn-App gescannt werden.</p> <p>2. Erklärungstext wird angezeigt.</p>

E06.02	Als App-Nutzer möchte ich innerhalb der Warn-App informiert werden, sobald ein Testergebnis verfügbar ist.	<ol style="list-style-type: none"> 1. Der App-Nutzer erhält eine Benachrichtigung, sobald ein verifiziertes Testergebnis vorliegt. 2. Die Benachrichtigung enthält nicht das Ergebnis positiv oder negativ.
E06.03	Als App-Nutzer möchte ich, dass bei Vorliegen meines positiven Testergebnisses nach meiner Zustimmung die pseudonymisierten IDs, auf deren Basis ich an den vergangenen Tagen für andere App-Nutzer sichtbar war, an den Warn-Server übermittelt werden, damit Kontaktpersonen durch Ihre Apps gewarnt werden können.	<ol style="list-style-type: none"> 1. IDs können pseudonymisiert an den Warn-Server übermittelt werden. 2. Übermittlung ist nur möglich, sofern zuvor eine Verifikation erfolgreich durchgeführt wurde. 3. Übermittlung ist nur möglich, sofern der App-Nutzer vorher zugestimmt hat.
E06.04	Als App-Nutzer möchte ich neben dem digitalen auch einen manuellen Prozess, z.B. über ein Call-Center nutzen können, damit auch ohne einen vorhandenen QR-Code die pseudonymisierten IDs, unter denen ich in den vergangenen Tagen für andere App-Nutzer sichtbar war, an den Warn-Server übermittelt werden, damit Kontaktpersonen durch Ihre Apps gewarnt werden können.	<ol style="list-style-type: none"> 1. Die zuständige Stelle kann eine TAN generieren und diese dem App-Nutzer mitteilen. (Generiert wird die TAN von einem Server, nicht durch das Call-Center selbst)
E06.05	Als App-Nutzer möchte ich die Möglichkeit zur Eingabe einer TAN innerhalb der App haben, damit ich die mir telefonisch mitgeteilte TAN zur Zuordnung meines Testergebnisses zu der von mir genutzten Instanz der App nutzen kann.	<ol style="list-style-type: none"> 1. Die Eingabe einer TAN innerhalb der App ist möglich. 2. Überprüfung und Rückmeldung, ob die eingegebene TAN korrekt war (zu prüfen, ob technisch möglich).
E06.06	Als App-Nutzer möchte ich, dass ich nach der Verifikation der TAN meine pseudonymen IDs freiwillig teilen und etwaige Kontaktpersonen warnen kann.	<ol style="list-style-type: none"> 1. IDs können pseudonymisiert an den Warn-Server übermittelt werden. 2. Übermittlung ist nur möglich, sofern zuvor eine Verifikation erfolgreich durchgeführt wurde. 3. Übermittlung ist nur möglich, sofern der App-Nutzer vorher zugestimmt hat.

Parametrierung

# User Story ID	User Story	Akzeptanzkriterien
E07.01	Als RKI möchte ich die Parameter zur Risiko-Score-Bestimmung (im Rahmen der technischen Möglichkeiten durch die API) einstellen können, um stets den aktuellen Forschungsergebnissen zur Virusübertragung zu entsprechen.	<ol style="list-style-type: none"> 1. In Abhängigkeit von der bereitgestellten API können Schwellenwerte konfiguriert werden. 2. Die Anpassung wird auf den Endgeräten vorgenommen, ohne dass ein Update der App erforderlich ist.

Technische Unterstützung

# User Story ID	User Story	Akzeptanzkriterien
E08.01	Als App-Nutzer möchte ich eine Hotline kontaktieren können, um technische Probleme mit der Applikation zu lösen.	<ol style="list-style-type: none"> 1. Telefonnummer der technischen Hotline ist in der Applikation hinterlegt.

Barrierefreiheit

# User Story ID	User Story	Akzeptanzkriterien
-----------------	------------	--------------------

E09.01	Als App-Nutzer möchte ich eine Sprachausgabe nutzen können, um die Applikation (z.B. bei fehlendem oder eingeschränktem Sehvermögen) nutzen zu können.	1. Die Barrierefreiheit bzgl. Sprachausgabe wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.
E09.02	Als App-Nutzer möchte ich gute Kontraste, veränderbare Schriftgrößen und eine gut lesbare Schriftart haben, um die Texte der Applikation gut lesen zu können.	1. Die Barrierefreiheit bzgl. Kontraste und Schrift wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.
E09.03	Als App-Nutzer möchte ich, dass mir die Inhalte in einfacher Sprache zur Verfügung gestellt werden, damit ich leicht verstehe, wie ich die App nutzen kann und warum ich es tun sollte.	1. Die Barrierefreiheit wird im Rahmen des Content-Managements berücksichtigt.

Content Management

# User Story ID	User Story	Akzeptanzkriterien
E10.01	Als RKI möchte ich die Inhalte der Applikation zentral verwalten, um Aktualisierungen von Texten, Links, Hotlines etc. einmalig für alle Stellen in der App durchführen zu können.	<ol style="list-style-type: none"> 1. Das Content-Management erfolgt auf Grundlage der Anforderungen des RKI 2. Der Content wird auf statische und dynamische Inhalte entsprechend der technischen Machbarkeit differenziert 3. Aktualisierungen erfolgen in der ersten Version über ein App-Update.

Unterschriftfassung

**ANLAGE 6
ÄNDERUNGSVERFAHREN**

**ANLAGE 6
ÄNDERUNGSVERFAHREN**

Auftraggeber: _____
Vertragsnummern/Kennung Auftraggeber: _____
Auftragnehmer: _____
Vertragsnummern/Kennung Auftragnehmer: _____
Änderungsverfahren Nummer: _____

1 Auftraggeber verlangt folgende Änderungen des Leistungsumfanges (Change Request) (detailliert)

Ort _____ Datum _____ Unterschrift Auftraggeber (Name in Druckschrift)

2 Auftragnehmer prüft Änderungsverlangen (Innerhalb angemessener Frist)

Der Auftragnehmer lehnt das Änderungsverlangen ab, weil es für den Auftragnehmer unzumutbar ist.
Wesentliche Gründe: _____
Das Änderungsverfahren ist aus Sicht des Auftragnehmers beendet.

Der Auftragnehmer lehnt das Änderungsverlangen nicht ab.

- Die verlangte Änderung hat keine Auswirkungen auf Leistungszeitraum, Termine und Vergütung und Ziele des Projektvertrages. Der Auftragnehmer beginnt unverzüglich mit der Umsetzung des Änderungsverlangens.
- Die beantragte Änderung hat Auswirkungen auf Leistungszeitraum und/oder Termine und/oder Vergütung und/oder Ziele des Projektvertrages.
- Der Auftragnehmer weist den Auftraggeber auf folgende Auswirkungen des Änderungsverlangens hin: _____
und legt diese in folgendem Realisierungsangebot dar:
Angebotsbindefrist: _____ (Datum)
Realisierungsangebot:

Ort _____ Datum _____ Unterschrift Auftragnehmer (Name in Druckschrift)

**3 Auftraggeber entscheidet über Realisierungsangebot
(innerhalb Angebotsbindfrist)**

- Das Realisierungsangebot wird angenommen. Die Arbeiten werden auf der Grundlage des so geänderten Projektvertrages weitergeführt.
- Das Realisierungsangebot wird nicht angenommen. Die Arbeiten werden auf Basis des bisherigen Projektvertrages weitergeführt.

Ort _____

Datum _____

Unterschrift Auftraggeber (Name in Druckschrift) _____