



Leistungsbeschreibung & zusätzliche Bedingungen ANTIGEN-SCHNELLTEST-PORTAL– MVP VERSION

Impressum

Herausgeber

T-Systems International GmbH

Hahnstraße 43d

60528 Frankfurt am Main

WEEE-Reg.-Nr. DE50335567

nachfolgend – Telekom – genannt

<http://www.t-systems.de/pflichtangaben>/<http://www.telekom.de/pflichtangaben>

Copyright

© 2019 Alle Rechte, auch die des auszugsweisen Nachdruckes, der elektronischen oder fotomechanischen Kopie sowie die Auswertung mittels Verfahren der elektronischen Datenverarbeitung, vorbehalten.

INHALT

Impressum.....	2
Inhalt 3	
1 Einleitung	6
2 Einordnung in die CWA Gesamtarchitektur	6
2.1 Übertragung des Schnelltestergebnisses an den CWA Test Result Server.....	10
2.2 Abruf des Schnelltestergebnisses in die CWA App	11
2.3 Anzeige des Schnelltestergebnisses in der CWA App	13
2.4 Auslösen einer Warnung im Positiv-Fall.....	14
3 Funktionsbeschreibung	15
3.1 Administrationsbereich.....	15
3.1.1 Anlegen und Verwalten des Mandanten im System	15
3.1.2 Anlegen und Verwalten von Mandanten-Admin-Accounts.....	15
3.1.3 Anlegen und Verwalten von Nutzer-Accounts	15
3.1.4 Anlegen und Verwalten von Teststellen	15
3.2 Login / Zugang.....	16
3.2.1 Initial-Login / Aktivierung von Nutzer Accounts	16
3.2.2 Nutzer-Login (mit Zwei-Faktor-Authentisierung).....	16
3.2.3 Nutzer-Logout.....	16
3.3 Datenerfassung	17
3.3.1 Erfassung persönlicher Daten der Testperson	17
3.3.2 Erfassung der Testdaten.....	18
3.4 Proben-Identifikation.....	18
3.5 Speichern des Datensatzes	18
3.5.1 Datenübermittlung und Speicherung im Schnelltest-Portal Backend.....	18
3.5.2 Archivierung / Speicherung der Testergebnisse.....	21
3.5.3 Funktion zur Ermittlung des Testzeitpunkts.....	21
3.5.4 Returncodes zur Mitteilung der erfolgreichen Speicherung des Datensatzes	21
3.6 Anzeige des QR-Code für die CWA	21
3.7 Erfassen des Testergebnisses.....	22
3.7.1 Eingabe des Probenidentifiers (Proben-ID).....	22
3.7.2 Eingabe der Test-ID.....	22
3.7.3 Eingabe des Handelsnamens eines Tests	22
3.7.4 Eingabe des Testergebnisses.....	22
3.8 Persistieren des Testergebnisses	23
3.8.1 Funktion zum Invalidieren der Proben-ID.....	23

3.8.2	Persistieren des Testergebnisses in der Datenbank	23
3.9	Übermittlung des Testergebnisses an die CWA	23
3.9.1	Abfragelogik zur Übermittlung von Testergebnissen mit Einwilligung an die CWA	23
3.9.2	Programmlogik für REST-Anfragen zur Übermittlung der Test-ID und des Testergebnisses an die REST-Schnittstelle der Labordatenanbindung	24
3.10	Infektionsmeldung an das zuständige Gesundheitsamt (Positiv-Meldung)	24
3.10.1	Abfragelogik zur Ermittlung positiver Testergebnisse	24
3.10.2	Auswahl positiver Testergebnisse	24
3.10.3	Anzeige positiver Testergebnisse	24
3.10.4	Ausdruck positiver Testergebnisse	24
3.10.5	Download positiver Testergebnisse	24
3.11	Testdokumentation / KV-Abrechnung	25
3.11.1	Ermittlung und Anzeige durchgeführter Antigentests	25
3.12	Anzeige, Druck und Download von Testnachweisen	25
3.12.1	Abfragelogik zur Anzeige vorhandener Testergebnisse	25
3.12.2	Auswahl eines Testnachweises	25
3.12.3	Anzeige eines Testnachweises	26
3.12.4	Ausdruck eines Testnachweises	26
3.12.5	Download eines Testnachweises	26
3.13	Logging	26
3.14	Schnittstellen	26
4	Leistungen der Telekom	27
4.1	Bereitstellung	27
4.2	Betrieb	27
4.3	Servicelevel	27
4.3.1	Leistungsübergabepunkt	27
4.3.2	Service Verfügbarkeit	27
4.3.3	Ausgeschlossene Ereignisse	27
4.3.4	Hotline Services für die Anbindung von Schnelltestcentern an die Corona Warn App	28
4.3.5	Fehlerklassen / Prioritäten	29
4.3.6	Service Level Agreements (Reaktionszeiten)	29
4.3.7	Wartungsarbeiten	29
4.3.8	Schutz gegen Datenverlust	30
4.4	Leistungsänderungen	30
5	Mitwirkungspflichten des Partners	30
5.1	Datenschutzrechtliche Mitwirkungspflichten	30
5.2	Mitwirkungspflichten beim Onboarding und User Management	31
5.3	Mitwirkungspflichten bei der Nutzung des Schnelltest-Portals	31

5.4	Allgemeine Mitwirkungspflichten	32
5.4.1	Ansprechpartner	32
5.4.2	E-Mail-Kommunikation	32
5.4.3	Rechtskonformität	32
5.4.4	Missbrauchsverhinderung	32
5.4.5	Geheimhaltung von Zugangsdaten	33
5.4.6	Aufklärung von Sicherheitsvorfällen	33
5.4.7	Eventuell überlassene Einrichtungen der T-Systems	33
5.4.8	Störungen eventuell überlassener Einrichtungen der T-Systems	33
5.4.9	Erfüllungsgehilfen	34
5.4.10	Anzeige der Leistungsstörung bezüglich Mitwirkungspflichten	34
6	Glossar/ Abkürzungsverzeichnis.....	35

1 EINLEITUNG

Mit dem **CWA Schnelltest-Portal** stellt Telekom dem Teststellenbetreiber (Partner) eine sichere und datenschutzkonforme Web-basierte Software-Lösung für den Schnelltestprozess am Point of Care (PoC), inkl. der erforderlichen Dokumentations- und Meldepflichten, zur Verfügung. Diese Lösung ist als assoziiertes System mit dem Gesamtsystem der Corona-Warn-App (CWA) verbunden und unterstützt den Prozess zur Anzeige von Schnelltestergebnissen in der Corona-Warn-App.

Über eine solche Anbindung an das Corona-Warn-App-System kann eine zeitnahe Benachrichtigung der getesteten Person erfolgen, die im Fall eines positiven Ergebnisses zudem über den anonymen Warnmechanismus der App umgehend andere Nutzer warnen kann, zu denen im zurückliegenden Gefährdungszeitraum durch die CWA erfasste Kontaktintensität bestand.

Weiterhin soll durch die schnelle und vertrauenswürdige Anzeige von Testergebnissen in der CWA App, auf Wunsch auch personalisiert als Testnachweis, ein Anreiz zur Erhöhung der Testhäufigkeit durch die Bürgerinnen und Bürger gesetzt werden.

Dieses Dokument umfasst die Funktionalitäten der MVP-Version der Lösung (Minimum Viable Product). Nachfolgende Ausbaustufen sind vorgesehen.

Hinweise:

- Im CWA-Backend, dem CWA Server, werden weiterhin keine personenbezogenen Daten verarbeitet oder vorgehalten.
- Im assoziierten System des CWA Schnelltest-Portals ist es aus fachlichen und rechtlichen Gründen erforderlich personenbezogene Daten zu erheben und zu verarbeiten. Dies erfolgt unter Einhaltung höchster Sicherheits- und Datenschutzanforderungen

Systemvoraussetzungen:

- Die Portal-Website läuft auf jedem modernen Browser und mithin auf allen verbreiteten Betriebssystemen (Mindestversionen:
 - Chrome 49, 85 bis 90
 - Edge 89 bis 90
 - Firefox 87 bis 88
 - Internet Explorer 11
 - IOS Safari 12.2 bis 12.4, 13.4 bis 13.7, 14.0 bis 14.4
 - Opera 73, 75
 - Safari 8, 13.1, 14
 - Android ab 4.4
 - Samsung 13.0, 14.0)

2 EINORDNUNG IN DIE CWA GESAMTARCHITEKTUR

Die CWA ist ein Gesamtsystem aus verschiedenen Komponenten, bei dem keine personenbezogenen Daten im Backend gespeichert werden.

Die zentrale Komponente zur Nutzer-Interaktion ist die CWA App als mobile Applikation für Smartphones. Als native Applikation für iOS- und Android-Geräte nutzt sie für die Kernfunktionalität der Kontaktermittlung sowohl die Komponenten als auch zusätzliche Bibliotheken des jeweiligen

Betriebssystem und des von Apple und Google bereitgestellten Exposure Notification Framework (ENF). Das ENF stellt eine Systemkomponente des Betriebssystems bzw. der bereitgestellten Software-Bibliotheken dar.

Für die Verschlüsselung der Daten, wie auch für das Anzeigen von Benachrichtigungen, werden ebenfalls Betriebssystemkomponenten verwendet. Für das Auslesen eines QR-Codes wird die zxing QR-Code Library verwendet; diese nutzt wiederum die betriebssystemseitige Kamerakomponente bzw. Kameraschnittstelle. Bei der Kommunikation mit den Serverkomponenten der CWA verwendet die CWA App die Protobuf-Bibliothek.

Der CWA Server dient als Server-Komponente der CWA App und hat als Kernaufgabe die Verwaltung bzw. Verteilung von Schlüsselinformationen sowie Check-Ins von positiv getesteten Nutzern in Form von Positivschlüssel-/Check-In-Paketen.

Für die Speicherung hochgeladener Positivschlüssel und Check-Ins von positiv getesteten Nutzern wird ein eigener Storage Service genutzt. Dieser wird vom CWA Server bespielt und vom Content Delivery Network (CDN) als zentrale Datenverteilungsquelle genutzt. Der Storage Service ist Teil des CDN.

Das Content Delivery Network der Telekom dient zur Bereitstellung von Datenpaketen mit den Positivschlüsseln und der Check-Ins der positiv getesteten Nutzer sowie des Poster Templates. Der Storage Service dient dem CDN als Quelle der Auslieferung von Daten an die CWA Apps welche aktiv die Daten anfragen. Für die Bereitstellung der Schlüssel und Check-Ins über das CDN werden keine Push-Benachrichtigungen genutzt. Die Abfrage der Schlüssel und Check-Ins erfolgt durch die CWA App (auch im Hintergrundbetrieb) beim CDN. Somit wird ausgeschlossen, dass Drittanbieter (z. B. von Push-Notification-Netzwerken) von der Nutzung der CWA App oder dem Inhalt von Positivschlüssel-Paketen sowie Check-Ins Kenntnis nehmen können.

Der Verifikationsserver dient als zentrale Komponente zur Verifikation von Daten im Rahmen der CWA. Er generiert und speichert alle gültigen Registration Token, die zum Abrufen von Testergebnissen im QR-Code-Verfahren notwendig sind. Ebenso stellt er Prüfdienste zur Verfügung, welche vom CWA Server genutzt werden, um sicherzustellen, dass nur positiv getestete Nutzer ihre Positivschlüssel hochladen können und es somit nicht zur Fehlalarmen kommt.

Der CWA Test Result Server hat im Rahmen der CWA die Aufgabe, die von den Laboren weitergeleiteten Testergebnisse zu registrierten Tests entgegenzunehmen. Der CWA Test Result Server speichert die eingehenden Testergebnisse und stellt die Verknüpfung zu den CWA Test IDs her, welche per QR-Code gescannt wurden. Nur Informationen zu Tests, bei denen der QR-Code gescannt wurde, werden hier gespeichert. Der CWA Test Result Server dient als reines Datenspeicherungssystem. Die gespeicherten Testergebnisse werden dem Verifikationsserver zum Abruf bereitgestellt.

Weitere Informationen siehe die Open-Source veröffentlichten Dokumente, insbesondere:

- a die Open Source veröffentlichte CWA Dokumentation: <https://github.com/corona-warn-app/cwa-documentation>
- b den Bericht zur Datenschutzfolgenabschätzung für die Corona-Warn-App: <https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf>

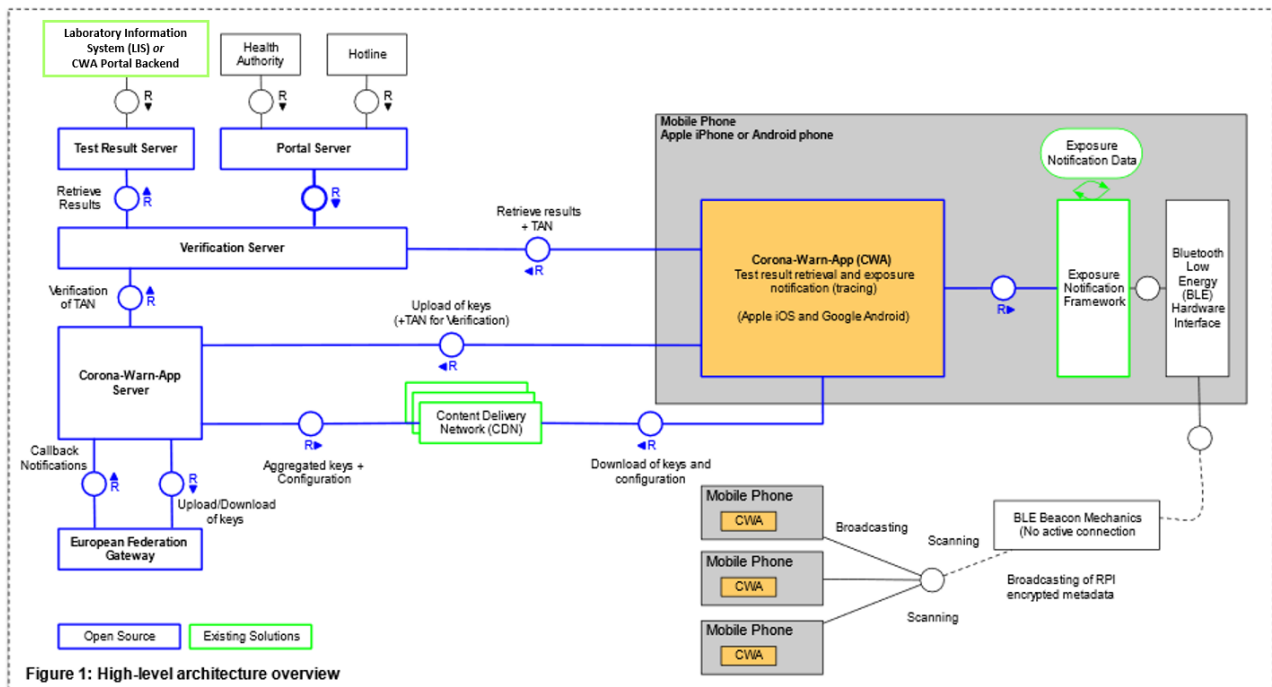


Abbildung 1: High Level Architecture - Fokus auf Komponenten

Die Integration in das Gesamtsystem der CWA untergliedert sich aus der Perspektive der Übergabe eines Schnelltestergebnisses aus dem Schnelltest-Portals in vier Funktionen:

- 1 Die Übertragung des Schnelltestergebnisses an den CWA Test Result Server
- 2 Den Abruf des Schnelltestergebnisses in die CWA-App
- 3 Die Anzeige des Schnelltestergebnisses in der CWA-App
- 4 Das Auslösen einer Warnung im Positiv-Fall

Sie erfolgt gemäß folgender System-Architektur:

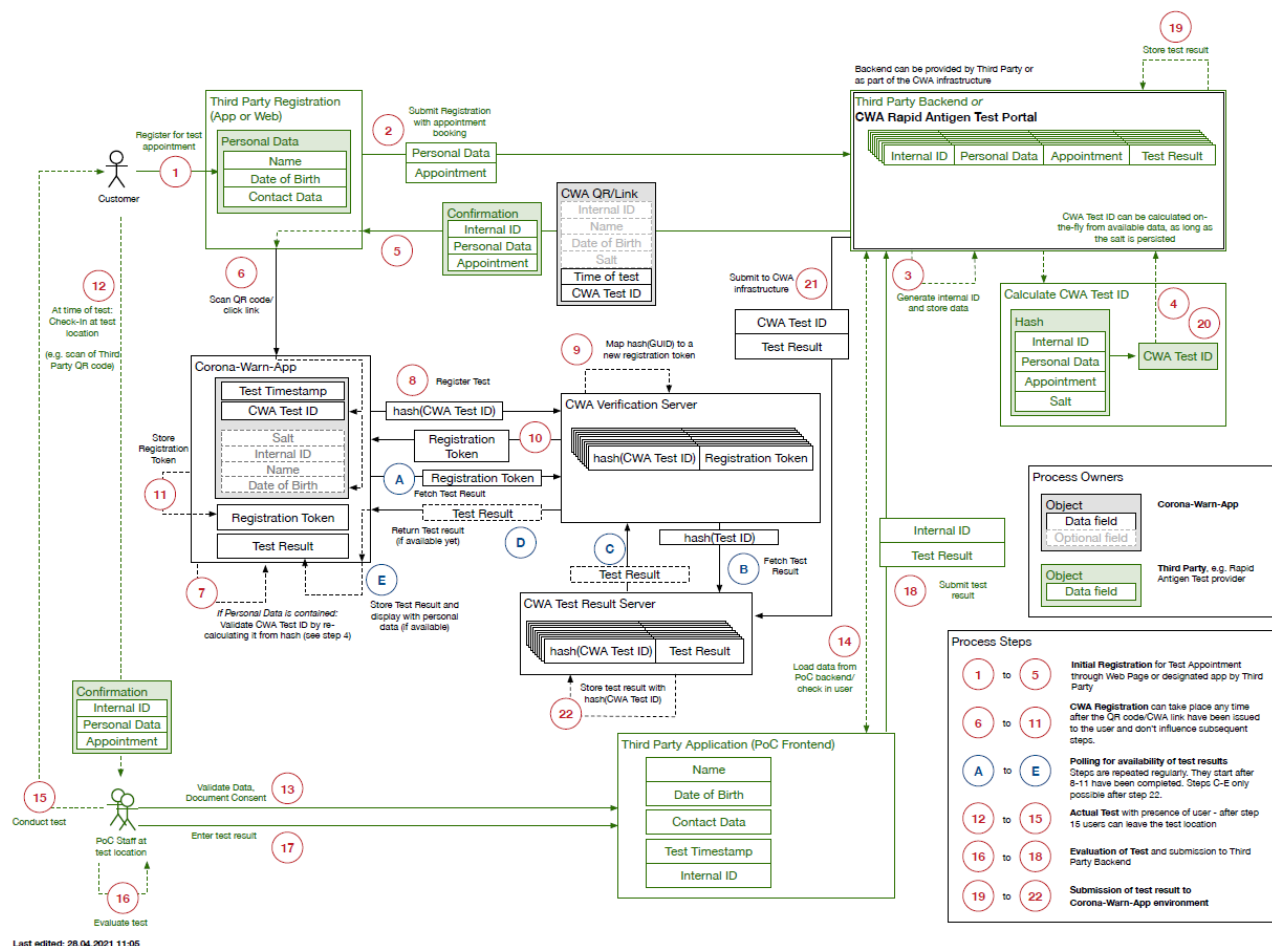


Abbildung 1: Architektur CWA Schnelltest-Integration (Ende-zu-Ende Darstellung)

Voraussetzungen zur Nutzung durch den Partner sind:

- Eine ausreichende Internetverbindung der Teststelle(n) des Partners
- Weitere Mitwirkungsleistungen (s. die in der Leistungsbeschreibung bezeichneten Mitwirkungspflichten)

Voraussetzungen zur Nutzung durch eine Testperson sind:

- Die Installation der CWA-App auf dem mobilen Endgerät der Testperson.
- Die Nutzung von Smartphones mit iOS oder Android Betriebssystem neuerer Version:
 - Apple Smartphones mit iOS Betriebssystem:
Mit der Corona-Warn-App Version 1.12 werden zusätzlich auch die älteren iPhone Modelle iPhone 5s, iPhone 6, und iPhone 6 Plus unterstützt. Voraussetzung ist auf diesen Geräten das iOS Betriebssystem mindestens auf die Version iOS 12.5 zu aktualisieren.
Apple stellt für die Modelle iPhone SE (1. Generation), iPhone 6s, und neuere Modelle die Betriebssystem-Version iOS 13.7 und höher bereit.
 - Smartphones mit Android Betriebssystem:
Erforderliche Android-Version 6.0 oder höher
- Die Nutzung eines durch den Partner an die Testperson übergebenen QR-Codes oder App-Links, mit dem die Verbindung zwischen lokaler CWA-App und CWA Test-Result-Server ermöglicht wird
- Eine zur Datenübertragung ausreichende Internetverbindung des mobilen Endgeräts der Testperson/des CWA-Nutzers.

2.1 Übertragung des Schnelltestergebnisses an den CWA Test Result Server

Die Übertragung der Schnelltestergebnisse aus dem CWA Teststellen-Portals an das CWA-System erfolgt vereinfacht dargestellt nachfolgender System-Architektur:

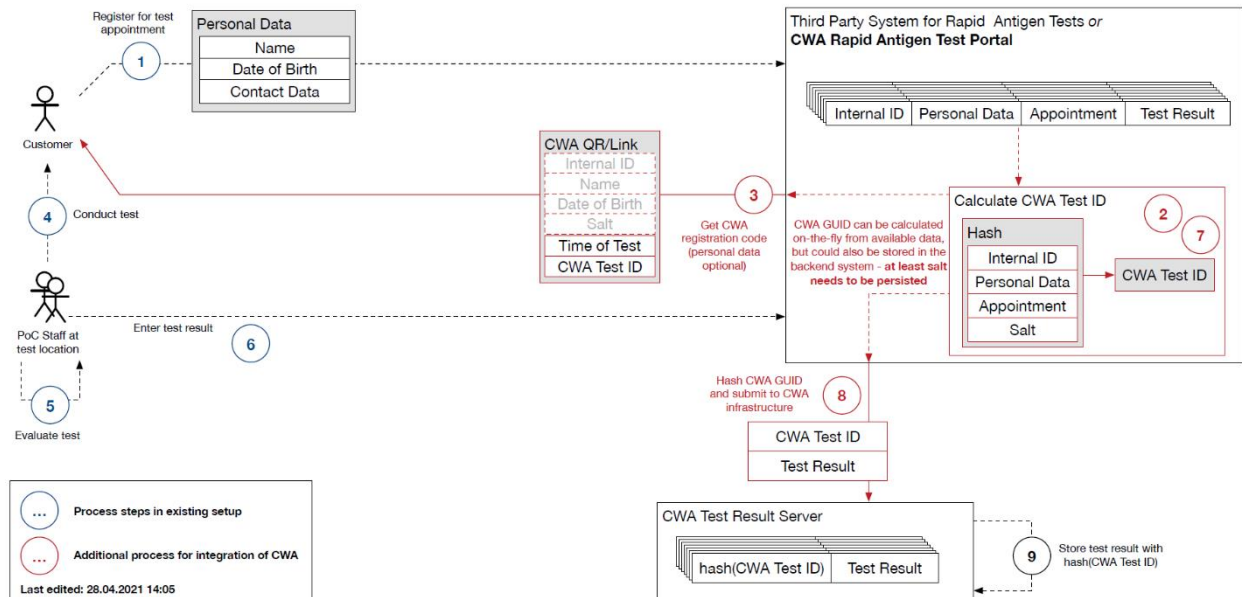


Abbildung 2: Architektur CWA Schnelltest-Integration (vereinfachte Darstellung)

Rechtliche Grundlage der Übertragung und des Ablegens des Testergebnisses auf dem CWA Test Result Server ist das Vorliegen einer Einwilligung zur Datenverarbeitung, die eine Testperson gegenüber dem Teststellenbetreiber abgibt.

Weiterhin ist eine Entscheidung der Testperson erforderlich, ob sie das Testergebnis später in der CWA-App unter Angabe der personenbezogenen Daten „Vorname“, „Nachname“, „Geburtsdatum“ angezeigt bekommen möchte, oder die Anzeige ohne personenbezogene Daten gewünscht wird.

–Die Integration des QR-Codes erfolgt vor Ort bei der Anmeldung in der Teststelle

- Der Mitarbeiter des Testzentrums gibt bei der Anmeldung der Testperson die persönlichen Daten über das Frontend der Teststellensoftware ein.
- Gleichzeitig wird auch die Einwilligung, zur Anzeige des Testergebnisses in der CWA App (mit oder ohne persönliche Daten) abgefragt und in der Eingabemaske vermerkt.
- Die Teststellen-Software des Partners generiert einen QR-Code, der im Web-Frontend angezeigt wird, oder einen App-Link, der in der genutzten App auf dem Smartphone angezeigt wird.
- Die Testperson scannt über die CWA App den QR-Code bzw. klickt in der Partner-App den angezeigten Link an, um die CWA App zu öffnen.
- Die Übertragung des Testergebnisses erfolgt nachfolgend über die Backend-Schnittstelle der Teststellensoftware des Partners an den CWA Test Result Server.

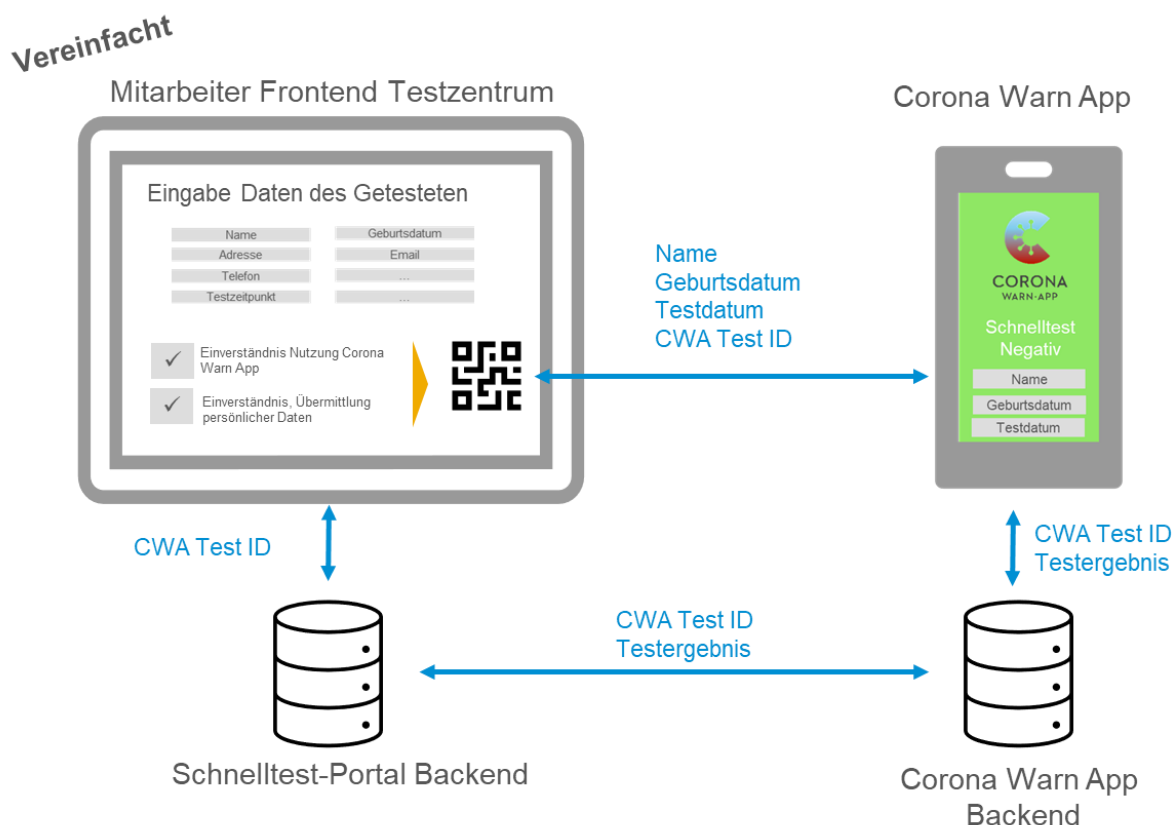


Abbildung 4: Die Integration des QR-Code erfolgt bei der Anmeldung im Testzentrum

2.2 Abruf des Schnelltestergebnisses in die CWA App

Voraussetzung zur Übertragung des Schnelltestergebnisses an die CWA App auf dem Smartphone der Testperson für die dortige Anzeige und ggf. Nutzung des dortigen Warnmechanismus ist der aktive Abruf des Schnelltestergebnisses von der CWA App beim CWA Test Result Server.

Die Verifikation zur Übergabe des Testergebnisses vom CWA Test Result Server an die CWA-App erfolgt über den Abgleich des CWA Test ID durch den CWA Verification Server. Dafür erfragt die CWA App mittels eines Registration Token beim Verifikationsserver das Vorliegen eines Testergebnisses. Der Verifikationsserver verwendet den Hashwert der CWA Test ID zur Abfrage, ob ein Testergebnis auf dem CWA Test Result Server für den CWA-Nutzer gespeichert ist.

Liegt ein Testergebnis unter dem Hashwert der CWA Test ID auf dem CWA Test Result Server vor, sendet der CWA Test Result Server dieses Testergebnis an den Verifikationsserver, der dieses seinerseits ohne Zwischenspeicherung das Ergebnis als positiven Befund, negativen Befund oder fehlerhafte Information an die CWA App überträgt.

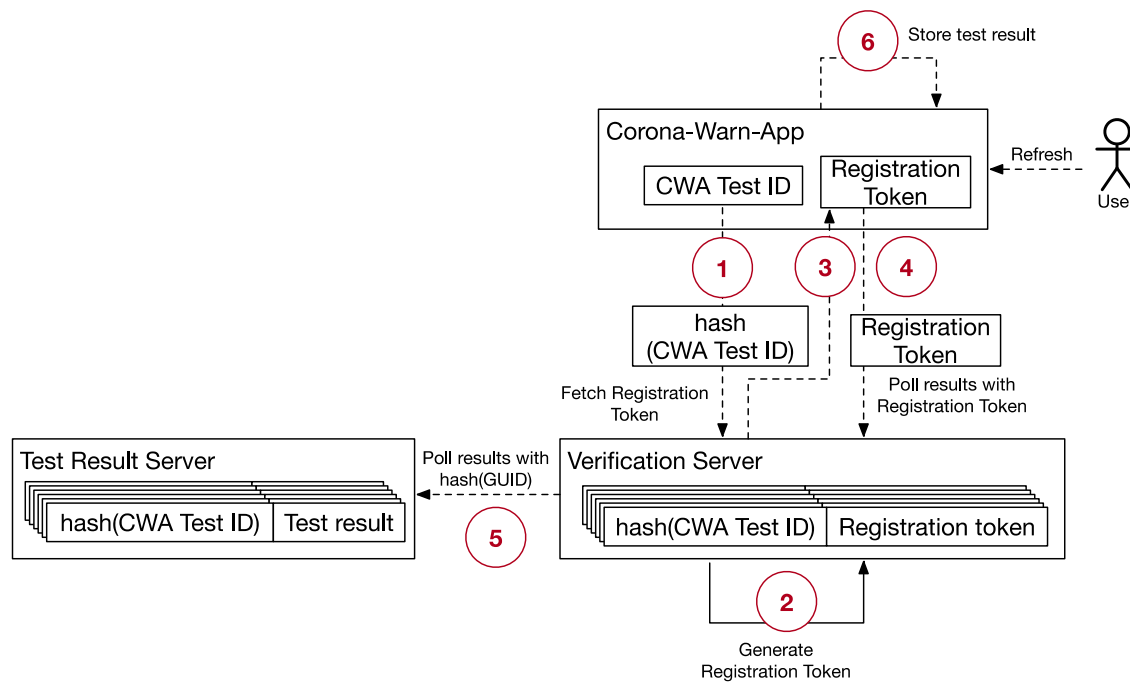


Abbildung 5: Abruf des Testergebnisses (vereinfachte Darstellung)

Technische Beschreibung:

- (1) Die CWA App extrahiert die CWA Test ID aus dem vorher eingelesenen QR-Code
- (2) Die CWA App bildet den Hashwert sha256 der CWA Test ID und überträgt diesen an den CWA Verification Server.
- (3) Der CWA Verification Server erzeugt einen Registration Token und überträgt diesen an die CWA-App. Gleichzeitig wird der Hashwert der CWA Test ID mit zugehörigem Registration-Token als Wertepaar auf dem CWA Verification Server gespeichert.
- (4) Die CWA App fordert das Testergebnis mittels Registration Token beim CWA Verification Server an.
- (5) Der CWA Verification Server ermittelt anhand des Registration Token den zugehörigen Hashwert der CWA Test ID und fordert damit das Testergebnis beim CWA Test Result Server an.
Falls ein Ergebnis vorliegt: Rückgabe des Ergebnisses (positiv, negativ, fehlerhaft)
Falls kein Ergebnis vorliegt: Rückgabe einer Leermeldung
- (6) Das Testergebnis wird in der CWA App persistiert, um es auch offline verfügbar zu machen.

Bei der CWA Test ID handelt es sich um ein nicht-auflösbares Pseudonym, das außerhalb des Zugriffsbereichs des RKI oder Dritter liegt.

An das CWA-System wird lediglich ein Hash-Wert der CWA Test ID übertragen. Dieser Hash-Wert wird lokal in der jeweiligen CWA App-Instanz anhand einer mathematischen Funktion berechnet, die nur in eine Richtung (Berechnung des Hash-Werts aus der CWA Test ID) eindeutig ist.

Aus dem Hash-Wert kann also nicht die CWA Test ID errechnet und somit bspw. zur Identifikation einer bestimmten Instanz der CWA-App verwendet werden.

Die QR-Code-Repräsentationen der CWA Test ID befinden sich ausschließlich im Machtbereich des CWA-Nutzers und des Teststellenbetreibers.

2.3 Anzeige des Schnelltestergebnisses in der CWA App

Die Anzeige des Schnelltestergebnisses erfolgt in der CWA App auf dem Smartphone der Testperson, nach der Abruf und Übertragung gemäß der unter 2.1. und 2.2 geschilderten Verfahren.

Angezeigt werden:

- Vorname, Nachname der getesteten Person (optional bei entsprechender Auswahl/Einwilligung)
- Geburtsdatum (optional bei entsprechender Auswahl/Einwilligung)
- Testergebnis
- Zeitpunkt der Testdurchführung

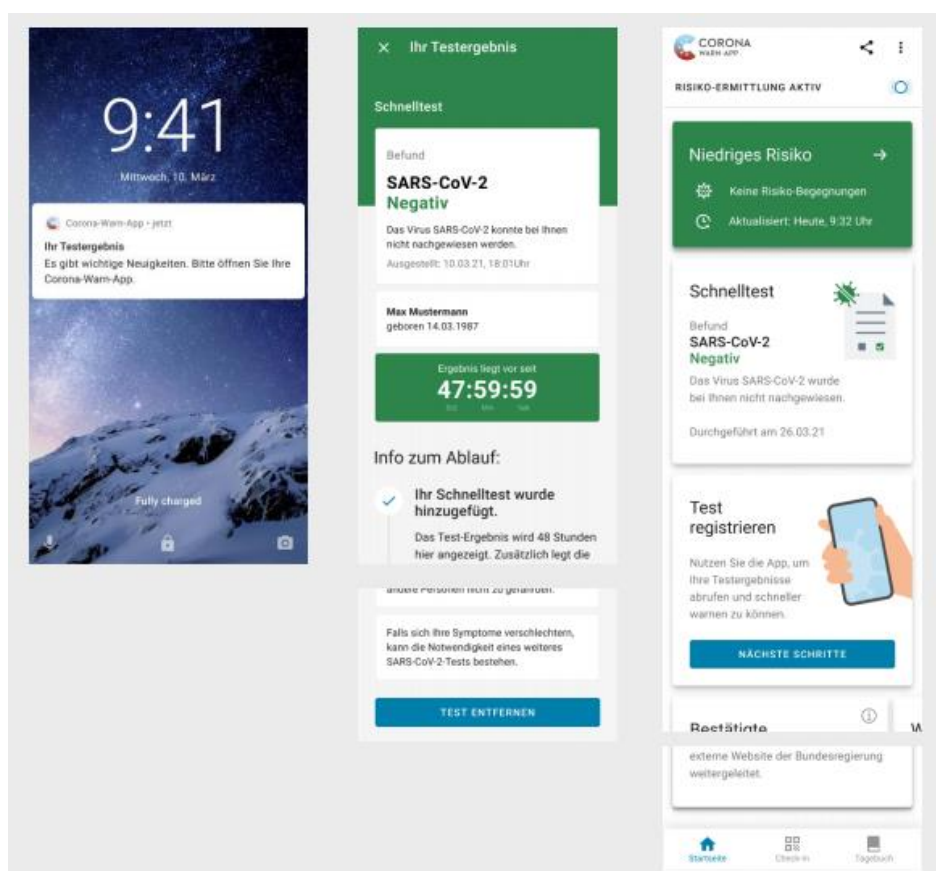


Abbildung 6: Screens in der CWA-App bei negativem Ergebnis (beispielhaft)

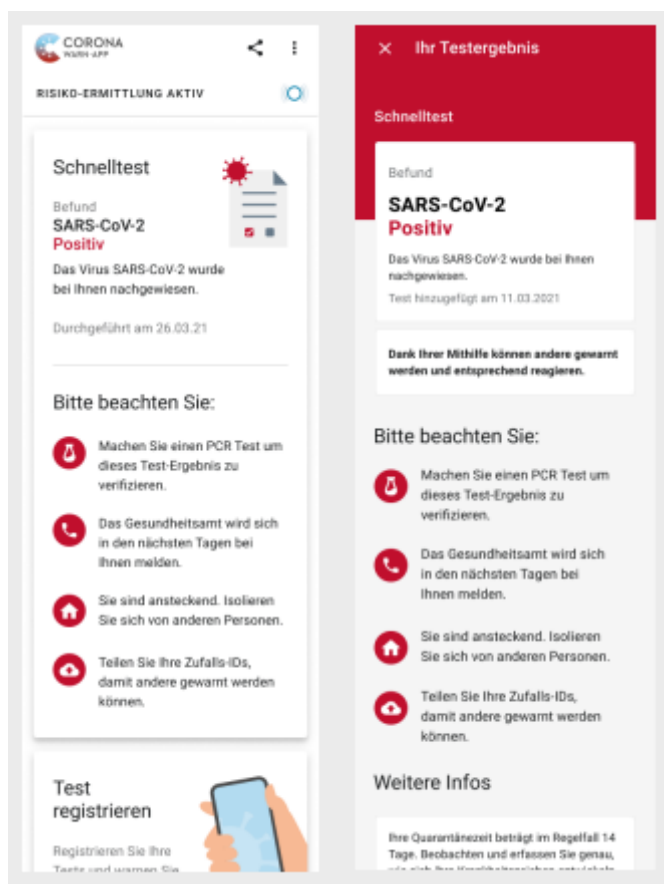


Abbildung 7: Screens in der CWA-App bei positiven Testergebnis (beispielhaft)

2.4 Auslösen einer Warnung im Positiv-Fall

Ein positiv getesteter CWA-Nutzer kann sein Testergebnis mit der Warnfunktion der CWA-App (auf dem Überblicks-Screen „Benachrichtigung anderer“ genannt) mit seinen Kontaktpersonen teilen und diese über eine mögliche Ansteckung informieren.

Technische Beschreibung:

Die Bereitstellung der Positivschlüssel eines positiv getesteten Nutzers erfolgt anonym mittels eines Verifikationsprozesses und einer einmaligen Transaktionsnummer (TAN).

Wenn ein positiv getesteter Nutzer seine Positivschlüssel bereitstellen will, so werden diese gemeinsam mit einer zuvor generierten TAN an den CWA Server geschickt. Dieser überprüft mit Hilfe des Verifikationsservers, ob die TAN gültig ist und sollte dies der Fall sein, werden die übermittelten Positivschlüssel vom CWA Server an den Storage Service des CDN weitergegeben.

3 FUNKTIONSBESCHREIBUNG

Das CWA Schnelltest-Portal in der aktuellen Ausbaustufe eines MVP (Minimum viable Product) umfasst die nachfolgend beschriebenen Funktionen.

3.1 Administrationsbereich

Die Verwaltung von Teststellenbetreibern, ihrer Teststellen sowie ihrer Mitarbeiter als Nutzer des Schnelltest-Portals erfolgt über einen Administrationsbereich. Das Schnelltest-Portal verwendet im dazugehörigen Backend das Tool "KeyCloak", wo mittels OpenID Connect die Nutzerauthentifizierung via Benutzername und Passwort durchgeführt wird. Bei erfolgreicher Authentifizierung erhält der Portal-Nutzer ein begrenzt gültiges Sitzungstoken, das zur Benutzung des Portal-Backends berechtigt. Nutzerverwaltung läuft direkt über einen mandantenfähigen KeyCloak-Account, der einem Administrator des Mandanten zur Verfügung gestellt wird.

Alle für die Verwaltung von Mandanten, Rollen, Accounts oder Nutzern notwendigen Funktionen sind bereits in der Grundfunktionalität von KeyCloak enthalten. Ein nachträgliches Editieren bzw. Löschen dieser Objekte ist möglich. Ebenso können auch einem Benutzer mehrere unterschiedliche Rollen zugewiesen werden.

3.1.1 Anlegen und Verwalten des Mandanten im System

Nach Vertragsabschluss legt Telekom für den Partner einen technischen Mandanten im Schnelltest-Portal System an, auf den nur von diesem benannte Mitarbeiter als Mandanten-Admin zugreifen können. Alle nachfolgend beschriebenen Accounts sind diesem Mandanten zugeordnet.

3.1.2 Anlegen und Verwalten von Mandanten-Admin-Accounts

Telekom legt für eine vom Partner benannte Auswahl von Mitarbeitern Mandanten-Admin-Accounts für dessen technischen Mandanten an. Die Mandanten-Admins verfügen über die Berechtigung, Accounts für weitere Mandanten-Admins (z.B. lokale Admins in den Teststellen) anzulegen sowie für die Mitarbeiter in den Teststellen (PoC), die für die Erfassung der Daten der Testpersonen und die Eingabe der Testergebnisse zuständig sind (im folgenden Nutzer genannt). Die Zugangsdaten (Nutzername + initiales Passwort) teilt Telekom den Mandanten-Admins des Kunden auf einem sicheren Weg mit.

3.1.3 Anlegen und Verwalten von Nutzer-Accounts

Der Admin-Bereich des Schnelltest-Portals ermöglicht dem Mandanten-Admin Accounts für Nutzer und ggf. weitere Mandanten-Admins anzulegen. Diesen sind nachfolgend die initialen Zugangsdaten (Nutzername + initiales Passwort) auf einem sicheren Weg mitzuteilen.

Der Mandanten-Admin hat die Berechtigung, die von ihm erstellten Accounts zu ändern und zu löschen.

3.1.4 Anlegen und Verwalten von Teststellen

Der Mandanten-Admin kann im System innerhalb seines Mandanten unterschiedliche Teststellen mit dazugehörigen Adressen anlegen, denen die dort durchgeführten Tests und dort tätigen Mitarbeiter (Nutzer) zugeordnet werden.

3.2 Login / Zugang

3.2.1 Initial-Login / Aktivierung von Nutzer Accounts

Ein Nutzer- oder Mandanten-Admin-Account wird mit der erstmaligen Anmeldung mit dem erhaltenen Nutzernamen und initialen Passwort aktiviert. Nachfolgend muss durch den Nutzer ein individuelles Passwort vergeben werden, das der von Telekom vorgegebenen Passwort-Richtlinie genügt.

Das Passwort muss mindestens 12 Zeichen aus mindestens drei der vier folgenden Klassen enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen

Für die bei späteren Anmeldevorgängen erforderliche Zwei-Faktor-Authentisierung (2FA) muss der Nutzer zudem initial eine Verbindung zwischen dem Account und einer 2FA-App auf seinem Smartphone herstellen, die One Time Passwords (OTP) erzeugen kann.

Für die Zwei-Faktor-Authentisierung kann der Nutzer z.B. eine der nachfolgenden Apps auf seinem Smartphone installieren und verwenden:

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

3.2.2 Nutzer-Login (mit Zwei-Faktor-Authentisierung)

Um Zugriff auf das CWA Schnelltest-Portal zu erlangen, muss sich jeder Nutzer mit seinem Nutzernamen, dem selbst vergebenen persönlichem Passwort sowie einem durch die vom Nutzer bei der Aktivierung des Accounts gewählte 2FA-App generierten 6-stelligen numerischen Einmal-Passwort (One-Time-Password, OTP) anmelden.

Nach erfolgreichem Login gelangt der Nutzer auf die Startseite, auf der ihm die für seine Rolle freigegebenen Funktionen angezeigt werden.

Auf der Loginseite (prä-Login) und innerhalb des CWA Schnelltest-Portals (post-Login) werden dem Tester jeweils Datenschutzhinweise zur Verfügung gestellt, in denen die Verarbeitung seiner personenbezogenen Daten im System beschrieben sind.

Alle Login-Versuche (erfolgreich und erfolglos) werden zusammen mit dem verwendeten Nutzernamen und der Zeitangabe gespeichert.

3.2.3 Nutzer-Logout

Der User kann sich über eine manuelle Logout-Funktion beim System abmelden. Bei einer Inaktivität von 30 Minuten erfolgt aus Sicherheitsgründen eine automatische Abmeldung (Timeout).

Gleichzeitig müssen die Anwender bezüglich des Nutzungsverhaltens geschult werden. Beim Verlassen des Arbeitsplatzes muss sich immer abgemeldet werden. Bei Nichtbeachtung kann der Nutzer zur Verantwortung gezogen werden.

3.3 Datenerfassung

3.3.1 Erfassung persönlicher Daten der Testperson

Für eine zweifelsfreie Zuordnung von Person und Testergebnis sowie zum Zwecke der Meldung von positiven Testergebnissen beim zuständigen Gesundheitsamt sowie zum Ausstellen einer Testbescheinigung ist im Schnelltest-Prozess die Erfassung personenbezogener Daten erforderlich sind.

3.3.1.1 Händische Eingabe über das Web-Frontend des CWA Schnelltest-Portals

Das Schnelltest-Portal bietet hierfür die Funktion „Patientendaten erfassen“, welche über das Hauptmenü des Portals aufzurufen ist.

Die Testperson identifiziert sich vor Ort anhand eines Ausweisdokuments, aus dem der Nutzer des Schnelltest-Portals die relevanten Daten (Name, Vorname, Geburtsdatum, Geschlecht, Adressdaten (PLZ, Ort, Straße, Hausnr.) übernimmt und zusammen mit Telefonnummer und E-Mail-Adresse in die Eingabemaske überträgt.

Im Zusammenhang mit der Datenerfassung und -verarbeitung werden auf der Erfassungsmaske über zwei Clickboxen folgende Einverständnisse dokumentiert:

- 1 Einwilligung zur Pseudonymisierten Übermittlung an die CWA (nicht-namentliche Anzeige des Testergebnisses in der CWA)**
„Das Einverständnis des Getesteten zum Übermitteln des Testergebnisses und des pseudonymen Codes an das Serversystem des RKI zum Zweck des Ergebnisabrufs in der Corona-Warn-App wurde erteilt. Es wurde darauf hingewiesen, dass das Testergebnis in der App hierbei nicht als namentlicher Testnachweis verwendet werden kann. Dem Getesteten wurden Hinweise zum Datenschutz ausgehändigt.“
- 2 Einwilligung zur personalisierten Übermittlung an die CWA (namentliche Anzeige des Testergebnisses in der CWA)**
„Das Einverständnis des Getesteten zum Übermitteln des Testergebnisses und des pseudonymen Codes an das Serversystem des RKI zum Zweck des Ergebnisabrufs in der Corona-Warn-App wurde erteilt. Der Getestete willigte außerdem in die Übermittlung von Namen und Geburtsdatum an die App zur Anzeige des Testergebnisses in der App als namentlicher Testnachweis ein. Dem Getesteten wurden Hinweise zum Datenschutz ausgehändigt.“

Die Datenschutzhinweise sind der Testperson zuvor in schriftlicher Form durch den Teststellenbetreiber auszuhändigen.

3.3.1.2 Scannen eines QR-Codes (vCard) der Testperson

Alternativ zur händischen Eingabe der persönlichen Daten der Testperson bietet das Schnelltest-Portal die Möglichkeit, erforderlichen personenbezogenen Daten über eine vCard in Form eines vorbereiteten QR-Codes zur Verfügung zu stellen. In diesem Falle wählt der Nutzer auf der Startseite des CWA Schnelltest-Portals die Funktion „QR-Code scannen“ und scannt den durch die Testperson über sein Smartphone vorgelegten QR-Code. Dies kann sowohl über einen angeschlossenen Handscanner sowie über die integrierte Kamera eines Rechners oder Tablets erfolgen.

Vor der Weiterverarbeitung sind die aus der vCard übernommenen Daten der Testperson durch einen Mitarbeiter der Teststelle mit dem vorgelegten Personalausweis der Testperson abzugleichen und auf Richtigkeit zu prüfen.

Zudem sind die unter 3.3.1.1 beschriebenen Vorgehensweisen zur Aushändigung von Datenschutzhinweisen und Einwilligungen vorzunehmen.

3.3.2 Erfassung der Testdaten

Die für den Ausweis in einem Testbeleg erforderlichen Angaben zum verwendeten Test (Test-ID und Handelsname) werden in der Eingabemaske zur Eingabe des Testergebnisses durch die Eingabe der Test-ID erfasst.

3.4 Proben-Identifikation

Zur eindeutigen Identifikation einer Testprobe ist eine Kennzeichnung dieser Testprobe erforderlich. Diese Kennzeichnung erfolgt über den zum Zeitpunkt der Erfassung persönlicher Daten der Testperson automatisch durch das Schnittstellen-Portal Backend erstellten 8-stelligen Probenidentifizier (Proben-ID). Die Proben-ID wird am rechten oberen Rand der Erfassungsmaske automatisch angezeigt und wird weiterhin für die spätere Eingabe des Testergebnisses sowie die Auswahl und Anzeige von Testbelegen benötigt. Die Proben-ID ist vom Nutzer im Testprozess händisch auf den Test zu übertragen.

Die Proben-ID wird aus den ersten 8 Stellen der im Schnelltest-Portal Backend erstellten CWA Test ID (Bei diesem Wert handelt es sich um einen mit SHA256 erzeugten 256 Bit Hashwert) gebildet. Die CWA Test ID wird dazu verwendet das Testergebnis ohne personenbezogene Daten, aber dennoch sicher und datenschutzkonform zuordnungsfähig, auf dem CWA Test Result Server abzulegen. Anzeige des Probenetiketts im Web-Frontend

3.5 Speichern des Datensatzes

3.5.1 Datenübermittlung und Speicherung im Schnelltest-Portal Backend

Das Schnelltest-Portal verfügt über ein eigenes Backend, in dem die Testergebnisse, die Kontaktdaten und die zugehörigen Test-IDs der Testpersonen sowie die Stammdaten der Mandanten, Teststellen und Nutzer gespeichert werden.

Via Proxy kommuniziert dieses Backend mit dem CWA Test Result Server (TRS) und leitet genau diejenigen Testergebnisse weiter, bei denen eine Einwilligung zur Weiterleitung zur CWA vorliegt.

Es werden folgende Daten aus dem Testprozess an das Schnelltest-Portal Backend übertragen:

Attribute	Type	Kommentar
Customer		
customer_first_name	text	„Max“
customer_last_name	text	„Mustermann“
customer_date_of_birth	YYYY-MM-DD	„1980-06-25“
customer_gender	single letter	"M" / "F" / "O" / "N" / "U" M stands for "male", F stands for "female", O stands for "other", N stands for "none or not applicable", U stands for "unknown"
customer_street_name	text	„Musterstraße“
customer_street_number	text	„17“
customer_postal_code	text	„65555“
customer_postal_town	text	„Musterstadt“
customer_country	text	„Deutschland“
customer_phon_number	text	„+49 190 1234567“
customer_eMail	text	„max@mustermann.de“
Flags		
flag_consent_rk_transfer	boolean	Flag (TRUE/FALSE) zur Einwilligung für die Übermittlung des Testergebnisses an die CWA (RKI Infrastruktur) „TRUE“
flag_pseudonym_QR-Code	boolean	Flag (TRUE/FALSE) für die Zustimmung der Patientendaten im QR-Code „FALSE“

Zu den verwendeten Testtypen und zum Testergebnis werden folgende Daten im Backend verarbeitet und gespeichert:

Attribute	Type	Kommentar
Antigen Test		
test_brand-ID	text	Test-ID des verwendeten Tests Handelsname (nach Bfarm Liste zugelassener Antigentests: https://antigen-test.bfarm.de/ords/f?p=101:100:31393141068255:::~&tz=2:00) „AT018/21“
test_brand_name	text	Antigentest Handelsname (nach Bfarm Liste zugelassener Antigentests: https://antigentest.bfarm.de/ords/f?p=101:100:31393141068255:::~&tz=2:00) „Cora Gentest-19“
salt	text	Generierte 128-Bit Zufallszahl in Hexadezimal-Darstellung, nur mit Großbuchstaben und fester Breite von 32 Stellen** (Das Salt ist notwendig, um daraus die CWA Test-ID zu generieren, welche wiederum zur Erzeugung des Ergebnis-PDF benötigt wird; daher muss dieser Wert so lange gespeichert werden wie der ganze Datensatz.)
test_sample-ID	text (8)	Die ersten 8 Zeichen der hash(CWA Test-ID) Proben-ID „67a50cba“ (Die Proben-ID wird im Dateinamen des Ergebnis-PDFs verwendet, muss also zur Rekonstruktion dieses PDFs so lange gespeichert werden wie der ganze Datensatz.)
test_time	unix timestamp, seconds	Test-Datum und -Uhrzeit werden auf dem PoC-Backend gesetzt, um Manipulationen und Eingabefehler zu verhindern. (Dieser Zeitstempel wird zur Erzeugung des Ergebnis-PDFs benötigt, muss also so lange gespeichert werden wie der ganze Datensatz.)

test_result	intger (1)	Siehe Tabelle
test_hinweistext	text	Sollte das Ergebnis Ihres Antigen-Schnelltests positiv ausgefallen sein, begeben Sie sich bitte unverzüglich in die häusliche Quarantäne und informieren Sie Hausstandsangehörige und weitere nahe Kontaktpersonen. Kontaktieren Sie umgehend Ihren Hausarzt oder die Leitstelle des Ärztlichen Bereitschaftsdienstes unter der Nummern 116 117 für weitere Verhaltensregeln und zur nun benötigten Durchführung eines PCR-Tests. Bitte beachten Sie, dass auch ein negatives Ergebnis eine mögliche Infektion nicht vollständig ausschließen kann und lediglich eine Momentaufnahme darstellt.

Als weitere prozessrelevante Datensätze werden folgende verarbeitet und gespeichert:

Attribute	Type	Kommentar
	Unique Identifier	
internal-ID	UTF-8 (35 Zeichen)	generierte UUID Typ 4 oder eine eigene ID* * Für das Attribut internal-ID wird eine UUID-Typ-4 empfohlen (128-bit Pseudo-zufallszahl). Anstelle der UUID Typ 4 kann vom Partner auch eine eigene Test-ID verwendet werden, diese ist in JSON als Zeichenkette zu behandeln.
CWA_Test-ID	Text	Wenn der nicht-anonymisierten Übermittlung des Testergebnisses an die CWA zugestimmt wurde, bildet sich die Test-ID durch SHA256([dob]#[fn]#[ln]#[timestamp]#[internal-id]#[salt]) Erklärung: <ul style="list-style-type: none"> • dob = date of birth (Geburtsdatum) • fn = first name (Vorname) • ln = last name (Nachname) • timestamp = test_time (s.o.) • internal-id = 128-bit UUID (s.o.) • salt = 128-bit salt (s.o.) Wenn nur der anonymisierten Übermittlung des Testergebnisses zugestimmt wurde, bildet sich die Test-ID durch SHA([timestamp]#[salt]) Auf diese Weise kann in beiden Fällen die Test-ID in der CWA durch Rehashing validiert werden, wodurch Betrugsversuche massiv erschwert werden. Dieser Wert wird nur für 14 Tage gespeichert.
Hash(CWA_Test-ID)	Text	Dies ist die gehashte CWA_Test-ID, die noch ein zweites Mal mit SHA-256 gehasht wurde (Doppel-Hashing). Dies ist notwendig, um denselben Ablauf beim Test Result Server verwenden zu können, wie er von den Laboren angewendet wird. Dieser Wert wird nur 14 Tage gespeichert.

Des Weiteren werden folgende Daten im Administrationsbereich verarbeitet und gespeichert:

Attribute	Type	Kommentar
	Mandant	
mandant-ID	text	Eindeutige ID, wird beim Anlegen des Mandanten von TSI Operation vergeben
mandant_name	text	„Quicktest Center GmbH“
mandant_street_name	text	„Musterweg“
mandant_street_number	text	„7“
mandant_postal_code	text	„45555“
mandant_postal_town	text	„Mustercity“
mandant_country	text	„Deutschland“
mandant_phone_number	text	„+49 140 1234567“

mandant_eMail	text	„info@quicktestcenter.de“
Point of Care		
poc-ID	text	Teststellen-ID ist nur eindeutig mit der Mandanten-ID. Diese ist eindeutig, wird vom Mandanten vergeben. Kann auch Freitext sein.
poc_name	text	Name der Teststelle „Teststelle Mustercity Musterweg 7“
poc_street_name	text	„Musterweg“
poc_street_number	text	„7“
poc_postal_code	text	„45555“
poc_postal_town	text	„Mustercity“
poc_country	text	„Deutschland“
poc_phone_number	text	„+49 140 1234567“
poc_eMail	text	„info@quicktestcenter.de“
poc_responsible_first_name	text	Verantwortlicher für Tests in Teststelle „Sabine“
poc_responsible_last_name	text	Verantwortlicher für Tests in Teststelle „Dr. Musterfrau“

3.5.2 Archivierung / Speicherung der Testergebnisse

Jedes gespeicherte Testergebnis wird nach 60 Tagen automatisch vom CWA Test Result Server gelöscht.

Auf dem Schnelltest-Portal Backend sind die Testergebnisse 14 Tage für die Portal-Nutzer des entsprechenden Mandanten, der den Test durchgeführt hat, abrufbar. Weiterhin werden die Daten wie gesetzlich gefordert für 10 Jahre stark verschlüsselt archiviert.

3.5.3 Funktion zur Ermittlung des Testzeitpunkts

Der Testzeitpunkt wird im Schnelltest-Portal Backend automatisch mit der Eingabe des Testergebnisses gesetzt.

3.5.4 Returncodes zur Mitteilung der erfolgreichen Speicherung des Datensatzes

Das Schnelltest-Portal Backend bestätigt die erfolgreiche Speicherung eines Datensatzes. Dies wird den Nutzern an den entsprechenden Stellen der Nutzeroberfläche angezeigt.

3.6 Anzeige des QR-Code für die CWA

Das Schnelltest-Portal generiert nach der erfolgreich abgeschlossenen Erfassung der persönlichen Daten der Testperson und der erforderlichen Einverständniserklärungen einen QR-Code zur Kopplung mit der Corona Warn App auf dem Smartphone der Testperson. Dieser QR-Code wird automatisch auf der Nutzeroberfläche des Schnelltest-Portals angezeigt.

Um eine Verbindung zwischen dem Testvorgang und der CWA App herzustellen muss lediglich der QR-Code mit dem Handy der Testperson in die CWA App eingelesen werden. Sobald später ein Testergebnis vorliegt kann dieses durch die CWA App abgerufen werden.

3.7 Erfassen des Testergebnisses

Nach Durchführung eines Schnelltests können die Nutzer in der Teststelle über das Hauptmenü die Funktion „Testergebnis erfassen“ anwählen und in einer entsprechenden Eingabemaske das Testergebnis zu einem Testvorgang eingeben.

3.7.1 Eingabe des Probenidentifiers (Proben-ID)

Um den Test eindeutig einem Vorgang und damit einer Testperson zuordnen zu können, ist die bei der Erfassung der personenbezogenen Daten automatisch vergebene Proben-ID (siehe 3.4 Probenidentifikation) in das zugehörige Feld einzugeben. Diese sollte zudem auf der Probe selbst vermerkt werden.

3.7.2 Eingabe der Test-ID

Um den Anforderungen an die Erstellung eines Testnachweises und der Meldung im Positiv-Fall zu genügen ist die Test-ID des für einen Test verwendeten Test-Typs (gemäß BfArM Liste zugelassener Antigentests) einzugeben.

3.7.3 Eingabe des Handelsnamens eines Tests

Um den Anforderungen an die Erstellung eines Testnachweises und der Meldung im Positiv-Fall zu genügen ist weiterhin der Handelsname des verwendeten Test-Typs (gemäß BfArM Liste zugelassener Antigentests) einzugeben.

3.7.4 Eingabe des Testergebnisses

Die Eingabe des Testergebnisses erfolgt über die in der Eingabemaske angezeigten Auswahlmöglichkeiten positiv / negativ / failed.

Speichern der Eingaben

Das Testergebnis und die weiteren Eingaben werden mit Betätigung des Buttons „Daten übermitteln“ gespeichert.

Eingabe abbrechen

Durch Betätigung des Buttons „abbrechen“ kann der Eingabevorgang jederzeit ohne Speicherung der Daten beendet werden. Die Anzeige wechselt in das Hauptmenü der Schnelltest-Portals.

3.8 Persistieren des Testergebnisses

3.8.1 Funktion zum Invalidieren der Proben-ID

Die 4 Byte lange Proben-ID von jedem Test wird als Primärschlüssel der mandantenspezifischen Quicktest-Tabelle verwendet und existiert so lange, bis entweder ein Testergebnis hochgeladen wurde oder 24 Stunden vergangen sind. Wenn nämlich das PDF für einen Schnelltest erzeugt wird, wird der zugrundeliegende Eintrag aus der Quicktesttabelle nicht mehr benötigt. Datensätze der Quicktest-Tabelle, die älter als 24 Stunden sind, werden von einem Scheduler gelöscht.

3.8.2 Persistieren des Testergebnisses in der Datenbank

Wird zu einem angelegten Datensatz mit Namen, Adresse usw. das Testergebnis hochgeladen, wird ein PDF mit der Testzusammenfassung erzeugt und im mandantenspezifischen Quicktest-Archiv abgelegt. Die Vorhaltezeit im Quicktest-Archiv beträgt 14 Tage; so lange hat das PoC-Personal Zugriff auf ein erzeugtes PDF. Nach Ablauf der 14 Tage werden die Daten von einem Scheduler auf komplexe Weise verschlüsselt und in einem Langzeitarchiv abgelegt, das aus rechtlichen Gründen die Daten für 10 Jahre speichert.

Der Zugriff auf das Langzeit-Archiv befindet sich momentan in der Entwicklung. Dabei ist vorgesehen, dass die Daten auf Zeilen-Ebene verschlüsselt werden. In jeder Zeile befindet sich zusätzlich zu den verschlüsselten Elementen ein Klartext-Element aus 6 Zeichen, welches Test-Tag, Test-Monat und die ersten beiden Zeichen des Nachnamens der Testperson enthält. Auf diese Art und Weise wird die Möglichkeit geschaffen, nach den Test-Details einer Testperson zu suchen, ohne dass nicht-anonymisierte Daten persistiert werden müssen.

T-Systems ist berechtigt, dem Partner die Daten aus dem Langzeitarchiv einmalig zur Gänze zur Verfügung zu stellen, insbesondere zum Ende der Vertragslaufzeit. Hierdurch sind sämtliche Ansprüche des Kunden auf Zugriff auf das Langzeitarchiv erfüllt und T-Systems ist berechtigt, das Langzeitarchiv des Partners zu löschen.

T-Systems ist berechtigt, binnen einer angemessenen Übergangszeit nach Vertragsschluss einen Abruf von Daten aus dem Langzeit-Archiv in angemessener Art und Weise bereitzustellen. Darüber hinaus steht Partner kein Anspruch auf Zugriff auf das Langzeitarchiv zu.

3.9 Übermittlung des Testergebnisses an die CWA

Mit der Speicherung der Eingaben zum Testergebnis (siehe 3.7 Erfassung des Testergebnisses) wird das Testergebnis zusammen mit der CWA Test ID an den CWA Test Result Server übergeben.

Die CWA auf dem Smartphone der Testperson holt es dort über eine Polling-Funktion automatisch ab und stellt es in der App bereit.

3.9.1 Abfragelogik zur Übermittlung von Testergebnissen mit Einwilligung an die CWA

Wenn eine Einwilligung zur Übermittlung des Testergebnisses an die CWA gegeben wurde, so genügt dies zur Weiterleitung. Dabei ist es unerheblich, ob einer anonymisierten oder personenbezogenen Weiterleitung zugestimmt wurde. Die personenbezogenen Daten werden nicht über das CWA-Backend übermittelt, sondern über den QR-Code, den der Nutzer mit der CWA ein-scant.

3.9.2 Programmlogik für REST-Anfragen zur Übermittlung der Test-ID und des Testergebnisses an die REST-Schnittstelle der Labordatenanbindung

Im Falle einer Einwilligung wird *ausschließlich* die Test ID und das Testergebnis via HTTP POST an den CWA Test Result Server (TRS) übermittelt; in naher Zukunft kommen noch der Zeitpunkt der Probenentnahme und der Testergebniszeitpunkt dazu. Der CWA TRS berechnet den Hashwert der Test-ID und speichert diesen, nicht jedoch die ursprüngliche Test-ID.

3.10 Infektionsmeldung an das zuständige Gesundheitsamt (Positiv-Meldung)

Das Schnelltest-Portal unterstützt die gesetzlich vorgeschriebene Infektionsmeldung an das zuständige Gesundheitsamt in der MVP-Version zunächst über eine rudimentäre Auswahl- und Ausdruck- oder Downloadfunktion. Hierfür gelangt der Nutzer über die Auswahl des Bereichs „Testergebnisse“ des Hauptmenüs in eine Maske zur Selektion, Anzeige und Ausdruck oder Download von Testbelegen im PDF-Format.

Der Meldevorgang erfolgt in der MVP-Version des Schnelltest-Portals nicht automatisch und ist durch den Teststellenbetreiber in eigener Verantwortung sicherzustellen.

3.10.1 Abfragelogik zur Ermittlung positiver Testergebnisse

Bei der Auswahl „Testergebnis positiv“ und eines Datums in der zugehörigen Eingabemaske wird eine Liste aller Proben-IDs von positiven Testfällen des entsprechenden Tages angezeigt.

3.10.2 Auswahl positiver Testergebnisse

Mit dem Anklicken einer Proben-ID in der Liste wird der zugehörige Vorgang ausgewählt.

3.10.3 Anzeige positiver Testergebnisse

Mit der Auswahl einer Proben-ID wird der mit diesem Vorgang und der Testperson verknüpfte Testbeleg unter Angabe aller für eine Infektionsmeldung erforderlichen Angaben als PDF-Dokument auf dem Bildschirm angezeigt.

3.10.4 Ausdruck positiver Testergebnisse

Mit der Auswahl der Druckfunktion des PDF-Dokuments wird der Ausdruck auf dem mit dem verwendeten Endgerät verbundenen Drucker ausgelöst.

Die Einhaltung datenschutzrechtlicher Anforderungen im weiteren Umgang mit einem solchem Ausdruck liegt in der Verantwortung des Teststellenbetreibers.

3.10.5 Download positiver Testergebnisse

Mit der Auswahl der Speicherfunktion des PDF-Dokuments wird der Download auf dem verwendeten Endgerät ausgelöst.

Die Einhaltung datenschutzrechtlicher Anforderungen im weiteren Umgang mit einer solcher Speicherung liegt in der Verantwortung des Teststellenbetreibers.

3.11 Testdokumentation / KV-Abrechnung

Das Schnelltest-Portal unterstützt die Abrechnung eines Teststellenbetreibers gegenüber den zuständigen KV in der MVP-Version zunächst nur über eine rudimentäre Anzeige der für eine Abrechnung erforderlichen Angaben (Anzahl durchgeführter Tests sowie Anzahl positiver Test eines Tages)

Der Abrechnungsvorgang erfolgt nicht automatisch und ist durch den Teststellenbetreiber in eigener Verantwortung sicherzustellen.

3.11.1 Ermittlung und Anzeige durchgeführter Antigentests

Über die Maske Auswertung werden die akkumulierten Ergebnisse eines Testtages angezeigt. Im Einzelnen werden die folgenden Kennzahlen angezeigt:

- Anzahl durchgeführter Tests einer Teststelle (PoC)
- Anzahl positiver Tests einer Teststelle (PoC)
- Prozentwert der positiven Testfälle

Die Anzeige erfolgt in der MVP-Version des Schnelltest-Portals ausschließlich für den jeweiligen Tag, 00:00 bis 24.Uhr). Eine nachträgliche Anzeige für vorhergehende Tage ist in der MVP-Version zunächst nicht verfügbar.

3.12 Anzeige, Druck und Download von Testnachweisen

Das Schnelltest-Portal unterstützt zunächst über eine rudimentäre Auswahl-, Ausdruck- und Downloadfunktion für Testnachweise. Hierfür gelangt der Nutzer über die Auswahl des Bereichs „Testergebnisse“ des Hauptmenüs ist eine Maske zur Selektion, Anzeige und Ausdruck oder Download von Testbelegen im PDF-Format.

3.12.1 Abfragelogik zur Anzeige vorhandener Testergebnisse

In der Eingabemaske der Oberfläche „Testergebnisse“ ist die Auswahl aller Tests sowie selektierter Test nach den Kriterien „positiv“, „negativ“ oder „failed“ an einem über ein Datumsfeld auszuwählenden Tag (Testzeitraum“) möglich. Als Ergebnis wird eine Liste aller Proben-IDs angezeigt, deren Testvorgänge den ausgewählten Kriterien entsprechen.

Hinweis: Auf dem Schnelltest-Portal Backend sind die Testergebnisse 14 Tage für die Portal-Nutzer des entsprechenden Mandanten, der den Test durchgeführt hat, abrufbar.

Weiterhin werden die Daten wie gesetzlich gefordert für 10 Jahre stark verschlüsselt archiviert. Diese sind jedoch für die Nutzer nicht über die normale Nutzeroberfläche zugänglich, sondern ausschließlich über den Mandanten-Administrator anzufordern.

3.12.2 Auswahl eines Testnachweises

Mit dem Anklicken einer Proben-ID in der Liste wird der zugehörige Vorgang ausgewählt.

3.12.3 Anzeige eines Testnachweises

Mit der Auswahl einer Proben-ID wird der mit diesem Vorgang und der Testperson verknüpfte Testbeleg unter Angabe aller für eine Infektionsmeldung erforderlichen Angaben als PDF-Dokument auf dem Bildschirm angezeigt.

3.12.4 Ausdruck eines Testnachweises

Mit der Auswahl der Druckfunktion des PDF-Dokuments wird der Ausdruck auf dem mit dem verwendeten Endgerät verbundenen Drucker ausgelöst.

Die Einhaltung datenschutzrechtlicher Anforderungen im weiteren Umgang mit einem solchem Ausdruck liegt in der Verantwortung des Teststellenbetreibers.

3.12.5 Download eines Testnachweises

Mit der Auswahl der Speicherfunktion des PDF-Dokuments wird der Download auf dem verwendeten Endgerät ausgelöst.

Die Einhaltung datenschutzrechtlicher Anforderungen im weiteren Umgang mit einer solcher Speicherung liegt in der Verantwortung des Teststellenbetreibers.

3.13 Logging

Das Schnelltest-Portal Backend umfasst das folgende Logging:

- Auf WRU/PROD Audit-Log von MySQL-Datenbanktransaktionen, insb. Fehlermeldungen.
- Info-Logs umfassen Zugriffszeiten, GUID-Kollisionen, Benutzername, Test-Upload-Erfolg und PDF-Download-Erfolg.
- Fehler-Logs umfassen alle erkannten Ausnahmen, die u.a. das Funktionieren der Datenbank- und HTTPS-Transaktionen umfassen.
- Loggen des Nutzers und Mandanten bei Hochladen eines Ergebnisses

3.14 Schnittstellen

Das Schnelltest-Portal Backend verfügt über Ingress-Schnittstellen zur Überprüfung automatisch generierter Proben-IDs auf Kollisionen, zum Upload von einzelnen Kontaktinformationen, zum Upload von einzelnen Testresultaten und zum Download aller noch nicht endgültig archivierten Daten.

Weiterhin verfügt das Schnelltest-Portal Backend über eine Egress-Schnittstelle zur Weiterleitung der erforderlichen Daten an das CWA-Backend (Nutzungsvoraussetzung: vorliegender Zustimmung einer Testperson zur Weiterleitung).

4 LEISTUNGEN DER TELEKOM

4.1 Bereitstellung

Die Telekom stellt die in Abschnitt 3 beschriebenen Funktionen als Web-Anwendung aus der Telekom-Cloud zur Verfügung, soweit nicht Bestandteile der Corona Warn App und Anzeigen der Corona Warn App beschreiben werden.

Der Partner erhält Zugangsdaten für Mandanten-Admin-Accounts, mit denen er weitere Accounts für seine Mitarbeiter anlegen kann.

4.2 Betrieb

Die Telekom betreibt sowohl das unter Kapitel 3 beschriebene System CWA Schnelltest-Portal. Die Corona Warn App, deren Bestandteile und die Anzeige des Testergebnisses in der Corona Warn App stellen keine Leistungen der Telekom nach dieser Leistungsbeschreibung dar.

4.3 Servicelevel

4.3.1 Leistungsübergabepunkt

Die Verantwortung der Telekom endet am Leistungsübergabepunkt. Leistungsübergabepunkt der Telekom ist jeweils die Web-Anwendung am Eintrittspunkt des Rechenzentrums in das Internet.

4.3.2 Service Verfügbarkeit

Die Verfügbarkeit der Applikation beträgt jeweils 99% im Kalendermonat und wird wie folgt berechnet:

$$\frac{(\text{gesamteServiceminuten}) - (\text{gesamteAusfallminuten})}{\text{gesamteServiceminuten}}$$

Sie wird als Prozentsatz (Verfügbarkeits-Prozentsatz) ausgewiesen. Dabei bedeutet:

Ein Ausfall bedeutet, dass der Anwendungsfall Transport (s. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) teilweise oder gänzlich nicht ausgeführt werden kann.

Durch das Einstellen eines Support-Tickets innerhalb der Service-Support-Zeiten beginnt die Berechnung der Ausfallminuten und endet mit der Behebung der Störung.

Gesamte Serviceminuten: die gesamte Anzahl der Kalendermonatsminuten (Berechnung 60 Minuten multipliziert mit 24 Stunden mal der Anzahl der Kalendertage im Monat)

Gesamte Ausfallminuten: die Anzahl der Minuten innerhalb eines Kalendermonats, in der der gegebene Autonomous Logistics Service nicht verfügbar ist, abzüglich der ausgeschlossenen Ereignisse in Minuten.

4.3.3 Ausgeschlossene Ereignisse

Ausfallzeiten auf Grund eines der nachfolgenden Ereignisse bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt:

- Ausfälle aufgrund von Wartungsarbeiten
- Ausfälle aufgrund von Störungen auf Infrastrukturebene Auftraggeber-seitig oder Zulieferern des AG
- Störungen, Ausfälle und Probleme, die auf den Kunden, seine Mitarbeiter oder Vertreter zurückzuführen sind, insbesondere Ausfälle auf Grund einer Überschreitung der zur Verfügung gestellten Kapazitäten

Zeiten für ausgeschlossene Ereignisse gelten nicht als Ausfallzeiten und bleiben daher bei der Berechnung der Verfügbarkeit unberücksichtigt. Das Vorliegen eines ausgeschlossenen Ereignisses reicht aus.

4.3.4 Hotline Services für die Anbindung von Schnelltestcentern an die Corona Warn App

Die Hotline Services für die Anbindung der Corona Warn App Services beinhalten folgende Leistungsmerkmale:

- exklusive Support Rufnummer für alle Partner mit unterschriebenem Partnervertrag.
- First Level Support mit Annahme der Problem-Meldung, Analyse und ggfs. sofortige Lösung.
- sollte dies nicht möglich sein erfolgt die Weitergabe des Requests an den Second Level Support, von dieser Organisationseinheit erfolgt dann ein Rückruf beim Partner mit der Detailklärung und Lösung.
- sollte dies nicht möglich sein erfolgt ein Routing in den Third-Level Support (Hersteller).

Die Leistungen des Supports im Überblick:

Die Support Services für die Anbindung der Schnelltestzentren umfassen obengenannte Leistungs- und Servicemerkmale. Nach dem GOLIVE werden dem Auftraggeber umfassende Auswertungen und Optimierungsvorschläge aus dem laufenden Betrieb unterbreitet (Beschreibungen folgen später).

Fokus der Tätigkeit bildet die telefonische Unterstützung und Hilfestellung im Zusammenhang mit der Anbindung der Teststellen an die Corona-App oder des Portals. Technisch komplexe Unterstützungsleistungen auf der Partnerseite sowie onsite Einsätze bei den Partnern sind nicht vorgesehen.

Die Lösung der Incidents erfolgt auf Basis von Frequently Asked Questions, die ständig mit neu aufgetretenen Fehlerbildern ergänzt werden. Lösungen, die nicht einem Bereich zuzuweisen sind, werden durch eine Clearingstelle analysiert und bearbeitet, das Feedback läuft wiederum in den First Line Support und die FAQs.

Die Hotline wird 7 Tage / Woche von 06.00 bis 20.00 Uhr abgefragt, soweit diese Tage keine gesetzlichen Feiertage sind.

Die Leistungserbringung erfolgt nur im Zusammenhang der Anbindung der Schnelltestcentern mit der Corona App. Es werden keine medizinischen Fragen oder detaillierte Fragen zum Datenschutz beantwortet. In diesen Fällen wird auf geeignete, vom Auftraggeber zur Verfügung gestellte, Dokumentationen (z.B. Webseiten) oder Hotlines verwiesen. Ein Erfolg der Beratung wird durch den Auftragnehmer nicht geschuldet.

4.3.5 Fehlerklassen / Prioritäten

Priorität	Definition	Beschreibung und Beispiele
Prio 1	Ausfall der Plattform oder Ausfall von kritischen Services mit gravierenden Auswirkungen (Entwicklung und Produktion) Eine hohe Useranzahl ist von dem Ausfall betroffen (Ausfall gegenüber Endkunden/User)	Eine Störung sorgt für einen Totalausfall eines Webshops und in Folge dessen für Verluste. Die Entwicklungsplattform ist komplett ausgefallen
Prio 2	Teilausfall der Plattform oder Teilausfall von Services mit Einfluss auf das Auftraggebergeschäft Hauptfunktionen sind bedeutend eingeschränkt Schnellstmögliche Wiederherstellung ist erforderlich Wenige User sind betroffen	Eine Störung sorgt für einen Teilausfall eines Rechnerverbundes oder einer Nicht-Verfügbarkeit eines (einzelnen) Mikroservices / einer Webapplikation, dadurch kommt es zu wesentlichen operativen Einschränkungen bspw. Funktionseinschränkungen
Prio 3	Hauptfunktionen bleiben verfügbar Randfunktionen sind unterbrochen Der Vorfall ist ohne Verfügbarkeitseinschränkungen Sehr wenige bis keine User sind betroffen	IT-Probleme oder andere Services / Funktionen die zu Unterbrechungen im Hintergrund führen, oder zu unwesentlichen Unterbrechungen Bspw. kosmetische Fehler (Design / Layout)

4.3.6 Service Level Agreements (Reaktionszeiten)

Zeitraum von der Meldung des Fehlers bis zur ersten Reaktion und bis zur Wiederherstellung.

	Kritisch	Schwer	Leicht
Erste Reaktion*	≤ 1 Stunde	≤ 4 Stunden	≤ nächster Arbeitstag

4.3.7 Wartungsarbeiten

Da Wartungsarbeiten am CWA Schnelltest-Portal keine Unterbrechungen verursachen, brauchen diese daher nicht angekündigt zu werden.

Falls in Einzelfällen durch Wartungsarbeiten doch Unterbrechungen verursacht werden, wird die Telekom den Kunden proaktiv im Vorfeld informieren. Die Telekom ist hierbei bestrebt, Beeinträchtigungen durch Wartungsarbeiten möglichst gering zu halten.

Wartungsarbeiten gelten nicht als Ausfallzeiten und bleiben daher bei der Berechnung der Verfügbarkeit unberücksichtigt.

4.3.8 Schutz gegen Datenverlust

Backend und Frontend des CWA-Schnelltestportals werden in einer OpenShift-Umgebung der Open Telekom Cloud (OTC) gehostet, die alle modernen Schutzstandards erfüllt; siehe auch <https://open-telekom-cloud.com/de/sicherheit/datenschutz-compliance>.

4.4 Leistungsänderungen

Die Telekom behält sich einseitige Leistungsänderungen und Entgeltreduzierungen zu Gunsten des Kunden vor. Der Kunde erklärt sich mit diesen Anpassungen einverstanden.

In Abweichung zu dem vereinbarten Schriftformerfordernis wird die Telekom den Kunden über etwaige Anpassungen durch Übersendung aktualisierter Versionen der bestehenden Vertragsunterlagen per E-Mail informieren, welche die bestehenden Unterlagen ersetzen.

5 MITWIRKUNGSPFLICHTEN DES PARTNERS

Der Partner ist verpflichtet, die nachfolgend beschriebenen Mitwirkungspflichten zu erfüllen. Ein Entgelt oder ein Ausgleichsanspruch steht dem Partner für die Erfüllung der Mitwirkungspflichten nicht zu.

5.1 Datenschutzrechtliche Mitwirkungspflichten

Der Partner ist verpflichtet, die Einwilligung des Nutzers der Corona-Warn-App gemäß Artikel 6 Abs. 1 lit a) DSGVO und Artikel 9 Abs. 2 lit a) DSGVO zur Übermittlung des Testergebnisses des Nutzers der Corona-Warn-App an das Robert Koch-Institut zur Darstellung in der Corona-Warn-App einzuholen, bevor der Partner die jeweilige CWA Test ID und das Testergebnis an die Antigen-Schnelltest-Schnittstelle zu der Corona-Warn-App übermittelt.

Der Partner ist verpflichtet, dem Nutzer der Corona-Warn-App ausreichende Datenschutzhinweise zur Übermittlung an die CWA und zur Verarbeitung personenbezogener Daten im Schnelltest-System zu erteilen, die mindestens den Umfang der in der Anlage 3 „Datenschutz-Hinweis“ beispielhaft vorgesehenen Hinweise aufweisen. Zudem ist der Partner verpflichtet, jeder Testperson den Datenschutzhinweis gemäß Anlage 4 „Aufklärungshinweise zum Datenschutz“ zu erteilen.

Der Partner ist verpflichtet, dem Nutzer der Corona-Warn-App die Erklärung der Einwilligung zur Übermittlung des Testergebnisses des Nutzers der Corona-Warn-App an das Robert Koch-Institut zur Darstellung in der Corona-Warn-App mittels der in der Anlage 3 „Datenschutz-Hinweis“ vorgesehenen Einwilligungstexte zu ermöglichen. Hierzu muss der Partner dem Nutzer der Corona-Warn-App die Wahl zwischen den in den Einwilligungstexten beschriebenen verschiedenen Einwilligungen frei ermöglichen.

Der Partner ist verpflichtet, eine erklärte Einwilligung eines Nutzers der Corona-Warn-App entgegenzunehmen und so zu dokumentieren, dass die Erteilung der Einwilligung des Nutzers der Corona-Warn-App nachgewiesen werden kann.

Der Partner ist verpflichtet, die Erfassung und Verarbeitung personenbezogener Daten durch Mitarbeiter der Teststellen des Partners derart zu protokollieren, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem eingegeben oder verändert worden sind (Eingabekontrolle). Dies umfasst auch die Dokumentation der Erteilung der Datenschutzhinweise und die Erfassung der Einwilligungen. Der Partner ist aus diesem Grund verpflichtet, sicherzustellen, dass sich die Mitarbeiter der Teststellen des Partners so gegenüber dem Backend des Partners authentifizieren, dass die Verarbeitungsvorgänge den Mitarbeitern jeweils zuzuordnen sind und die Weitergabe oder der anderweitige Missbrauch von Zugangs- und Verarbeitungsmöglichkeiten durch Maßnahmen der Betriebsorganisation des Partners unterbunden wird.

5.2 Mitwirkungspflichten beim Onboarding und User Management

Der Partner stellt T-Systems zeitnah nach Vertragsabschluss eine Liste der Personen zur Verfügung, die Mandanten-Admin-Accounts erhalten sollen. Die benannten Personen müssen durch den Partner in die Lage versetzt werden, die mit der Zuteilung eines Mandanten-Admin-Accounts verbundenen Aufgaben und Sorgfaltspflichten erfüllen zu können.

Die Mandanten-Admins erstellen als Arbeitnehmer oder Erfüllungsgehilfen des Partners Nutzer-Accounts und ggf. weitere Mandanten-Admins und teilen den betreffenden Mitarbeitern die initialen Zugangsdaten (Nutzername + initiales Passwort) auf einem sicheren Weg mit. Der Partner ist gegenüber Telekom für die Sicherheit sämtlicher Zugangsdaten verantwortlich.

5.3 Mitwirkungspflichten bei der Nutzung des Schnelltest-Portals

Der Partner stellt den Mitarbeitern in den Teststellen geeignete Hardware für den Zugriff auf das CWA Schnelltest-Web-Portal zur Verfügung, z.B. einen Rechner mit installiertem aktuellen Web-Browser und Internetzugang, auf dem das Web-Portal aufgerufen werden kann.

Der Mitarbeiter der Teststelle ist verpflichtet, die Identität und die Korrektheit der angegebenen oder via vCard ans Portal übermittelten Daten einer Testperson anhand des Personalausweises oder vergleichbaren Ausweisdokuments zu überprüfen.

Alle Nutzer des Systems beim Partner einschließlich aller Mitarbeiter des Partners nutzen als zweiten Faktor für jede Authentisierung am System zusätzlich zu Nutzernamen + Passwort ein Einmalpasswort (OTP), das von einer Zwei-Faktor-Authentifizierungs-App auf ihrem Smartphone erzeugt wird. Die Applikation zur Erzeugung des OTP sollte nicht auf dem gleichen Gerät installiert

sein, mit dem der Zugriff auf das CWA Schnelltest-Portal erfolgt. Verwendbare Apps sind unter anderem:

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

Der Partner ist verpflichtet, die von T-Systems im Identity & Access Management (KeyCloak) vor-konfigurierten Sicherheitseinstellungen unverändert zu verwenden. Insbesondere darf der Partner die Passwortrichtlinien nicht ändern und die Zwei-Faktor-Authentifizierung für das Login nicht de-aktivieren.

5.4 Allgemeine Mitwirkungspflichten

5.4.1 Ansprechpartner

Der Partner ist verpflichtet einen qualifizierten und entscheidungsbefugten Ansprechpartner zu be-nennen und dessen Erreichbarkeit/Vertretung während der Vertragslaufzeit sicherzustellen.

5.4.2 E-Mail-Kommunikation

Der Partner erklärt sich mit dem unverschlüsselten Schriftwechsel per E-Mail einverstanden und wird stets eine aktuelle E-Mail-Adresse hinterlegen. Dem Partner ist bekannt, dass für die Leis-tungserbringung wesentliche Informationen, wie Zugangsdaten, Informationen zu Änderungen der Leistungen und der rechtlichen Bedingungen, sowie Rechnungen ausschließlich per Mail versen-det werden.

5.4.3 Rechtskonformität

Der Partner prüft eigenverantwortlich alle für ihn im Zusammenhang mit der Nutzung der Leistung relevanten und anwendbaren rechtlichen Vorschriften, Gesetze, Verordnungen und branchenspe-zifischen Bestimmungen und stellt deren Einhaltung sicher. Dazu zählen insbesondere auch die Einhaltung von Geheimhaltungsverpflichtungen, die z.B. aus einer beruflichen Tätigkeit herrühren.

5.4.4 Missbrauchsverhinderung

Der Partner stellt sicher, dass die Leistungen nicht missbräuchlich genutzt werden. Eine miss-bräuchliche Nutzung liegt insbesondere vor, wenn die Leistungen von Unbefugten verwendet wer-den, die Leistungen nicht zu den vorgesehenen Zwecken verwendet werden oder die Leistungen zur Verarbeitung unwahrer Angaben eingesetzt werden. Stellt der Partner eine missbräuchliche Nutzung fest oder bestehen für ihn Anhaltspunkte für die begründete Vermutung einer miss-

bräuchlichen Nutzung, wird der Partner T-Systems diese missbräuchliche Nutzung und die Anhaltspunkte unverzüglich mitteilen. Z.B. ist eine Verwendung des Portals außerhalb der Dienstzeit untersagt.

5.4.5 Geheimhaltung von Zugangsdaten

Der Partner ist verpflichtet, ihm von T-Systems zugeteilte Passwörter, Zugangsdaten und Zertifikate geheim zu halten, nur an berechtigte Dritte weiterzugeben, vor unberechtigt Zugriff zu schützen und soweit erforderlich zu ändern. Der Partner wird T-Systems unverzüglich bei Vorliegen von Anhaltspunkten, dass unberechtigte Dritte Kenntnis von Passwörtern oder Zugangsdaten erhalten haben, informieren.

5.4.6 Aufklärung von Sicherheitsvorfällen

Der Partner ist verpflichtet, T-Systems bei der Aufklärung von Sicherheitsvorfällen zu unterstützen und T-Systems die von T-Systems bezeichneten angemessenen Informationen, gegebenenfalls auch durch das Anstellen eigener Ermittlungen, zur Verfügung zu stellen. Sicherheitsvorfälle stellen Vorfälle dar, bei deren konkretem oder eventuellem Vorliegen die in dieser Leistungsbeschreibung beschriebenen Leistungen von Unbefugten verwendet werden können, die Leistungen nicht zu den vorgesehenen Zwecken verwendet werden können oder die Leistungen zur Verarbeitung unwahrer Angaben eingesetzt werden können. Dies umfasst auch Vorfälle, die vom Cyber Defense Center des Konzerns der Deutschen Telekom AG entdeckt werden.

Zu diesem Zweck stellt der Partner sicher, dass ein qualifizierter und entscheidungsbefugter Ansprechpartner für T-Systems zur Bearbeitung von Sicherheitsvorfällen erreichbar ist und benennt diesen Ansprechpartner.

5.4.7 Eventuell überlassene Einrichtungen der T-Systems

Der Partner ist verpflichtet, ihm überlassene Einrichtungen der T-Systems vor unberechtigt Zugriff und Beeinträchtigungen durch geeignete Maßnahmen zu schützen, diese pfleglich zu behandeln und die Angaben der Hersteller zu beachten.

5.4.8 Störungen eventuell überlassener Einrichtungen der T-Systems

Der Partner ist verpflichtet Störungen, Beeinträchtigungen der Leistungen oder Beschädigungen an den ihm überlassenen Einrichtungen der T-Systems unverzüglich mit einer nachvollziehbaren Schilderung der Fehlersymptome anzuzeigen.

Der Partner ist verpflichtet, T-Systems bei der Behebung einer Störung der Leistungen zu unterstützen. Insbesondere führt der Partner vor Aufgabe eines Tickets soweit möglich eine Prüfung der Erfüllung der Mitwirkungsleistungen und seiner eigenen betrieblichen Vorgänge durch, um auszuschließen, dass die Störungsursache in seinem Verantwortungsbereich liegt.

5.4.9 Erfüllungsgehilfen

Der Partner stellt die Erbringung erforderlicher Mitwirkungsleistungen durch seine Vertragspartner oder sonst dem Partner zuzurechnende Dritte sicher, die als Erfüllungsgehilfen des Partners tätig sind.

5.4.10 Anzeige der Leistungsstörung bezüglich Mitwirkungspflichten

Der Partner wird T-Systems unverzüglich in Textform darüber informieren, wenn er eine Mitwirkungspflicht nicht wie vereinbart erfüllen kann. Er wird die nicht oder nicht vollständig erbringbare Mitwirkungspflicht bezeichnen und den Umfang der Leistungsstörung angeben.

6 GLOSSAR/ ABKÜRZUNGSVERZEICHNIS

CDN	Content Delivery Network
CWA	Corona Warn App (Gesamtsystem, App mit dazugehörigem Server)
CWA App	Corona Warn App, nur der App Anteil
CWA Server	Corona Warn App, nur der Server Anteil
ENF	Exposure Notification Framework
GUID	Globally Unique Identifier
LIS	Laboratory Information System
MVP	Minimum Viable Product
PoC	Point of Care
OTC	Open Telekom Cloud
QR-Code	Quick Response Code
UUID	Universally Unique Identifier