Funktions- und Leistungsbeschreibung

SCHNELLTEST-PORTAL

STAND: 17.03.2022

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

INHALT

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.

Hinweise:

- Im CWA Ecosystem werden weiterhin keine personenbezogen 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:

- Voraussetzung für die Nutzung des webbasierten Portals ist die Verfügbarkeit internetfähiger Endgeräte und eines Internetanschlusses in der Teststelle. Der Zugang erfolgt über einen Webbrowser (z.B. Firefox, Internet Explorer, Microsoft Edge, Safari, etc.).
- Außerdem wird ein mit dem Internet verbundenes Smartphone benötigt, auf dem eine OTP-App zur Erzeugung eines Einmal-Passworts (One-Time-Password, kurz OTP) installiert ist. In den AppStores von Google und Apple können Sie dafür z.B. die FreeOTP, Google Authenticator oder Microsoft Authenticator App herunterladen.
- Für eine Erfassung der Patientendaten über die in der Corona-Warn-App erzeugte vCard ist es notwendig, dass das Schnelltestportal auf einem mit dem Internet verbundenen Gerät (Tablet, Smartphone) verwendet wird, das über eine interne Kamera verfügt.

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 Betriebssystems 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

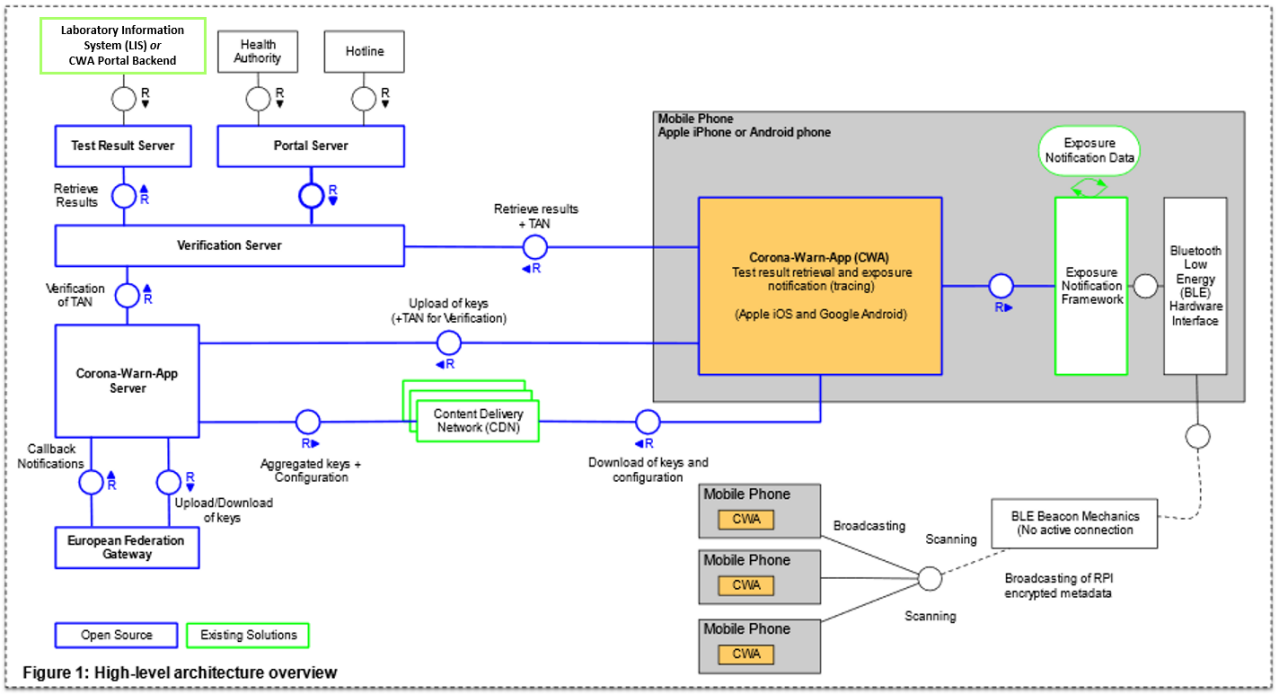

Abbildung 1: High Level Architecture - Fokus auf Komponenten

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:

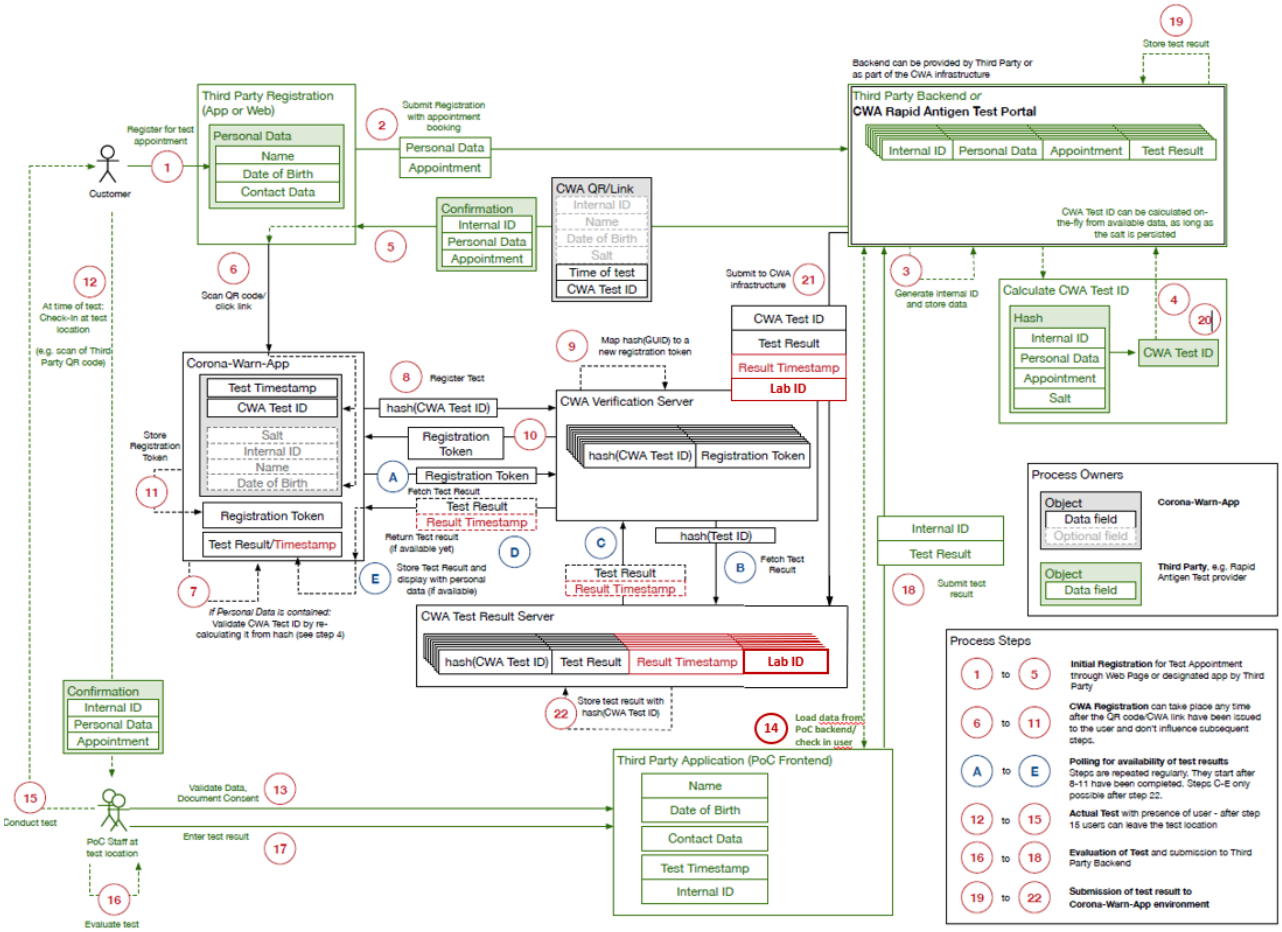

Abbildung 2: Architektur CWA Schnelltest-Integration (Ende-zu-Ende Darstellung)

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:

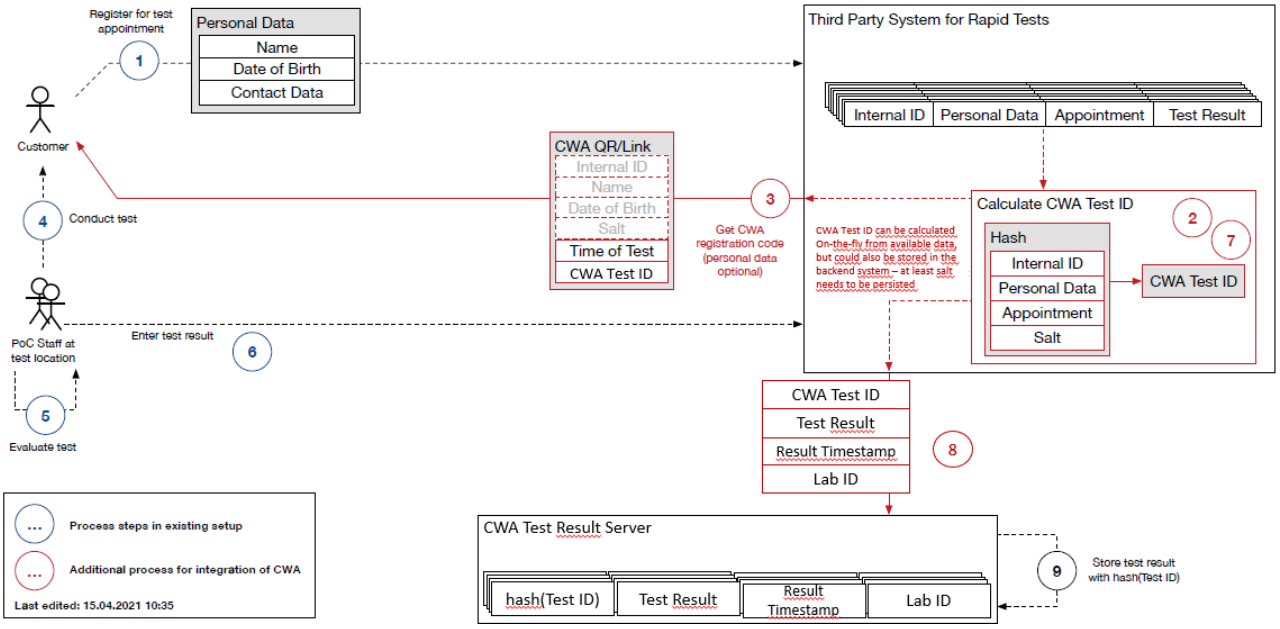

Abbildung 3: Architektur CWA Schnelltest-Integration (vereinfachte Darstellung)

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 Teststellen-Software 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 Teststellen-Software des Partners an den CWA Test Result Server.

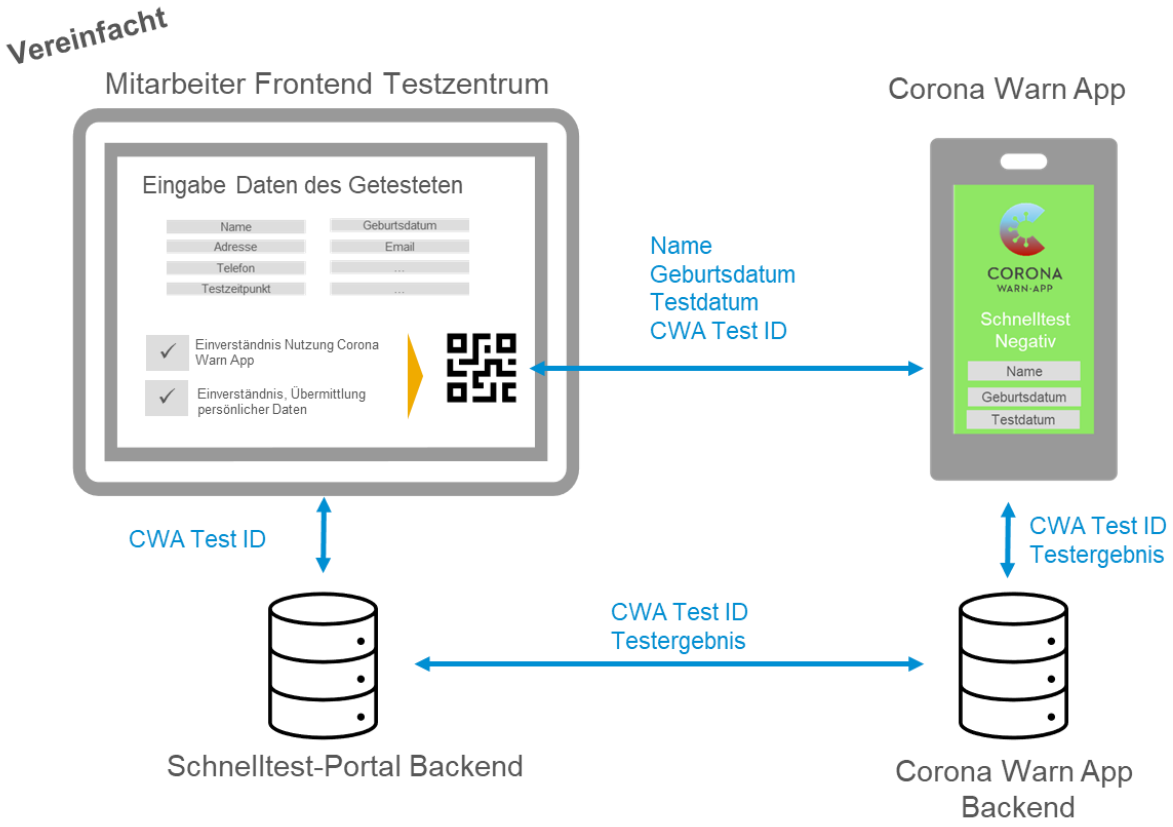

Abbildung 4: Die Integration des QR-Code erfolgt bei der Anmeldung im Testzentrum

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.

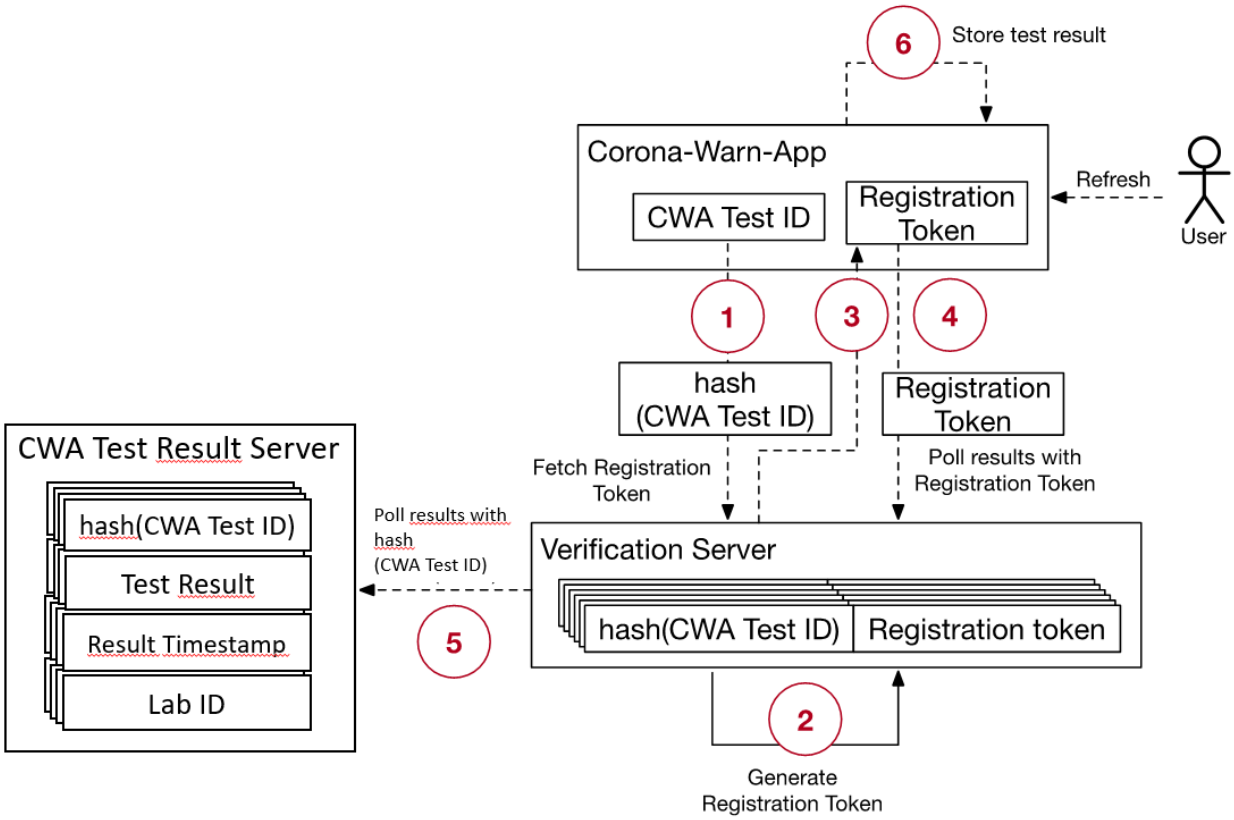

Abbildung 5: Abruf des Testergebnisses (vereinfachte Darstellung)

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

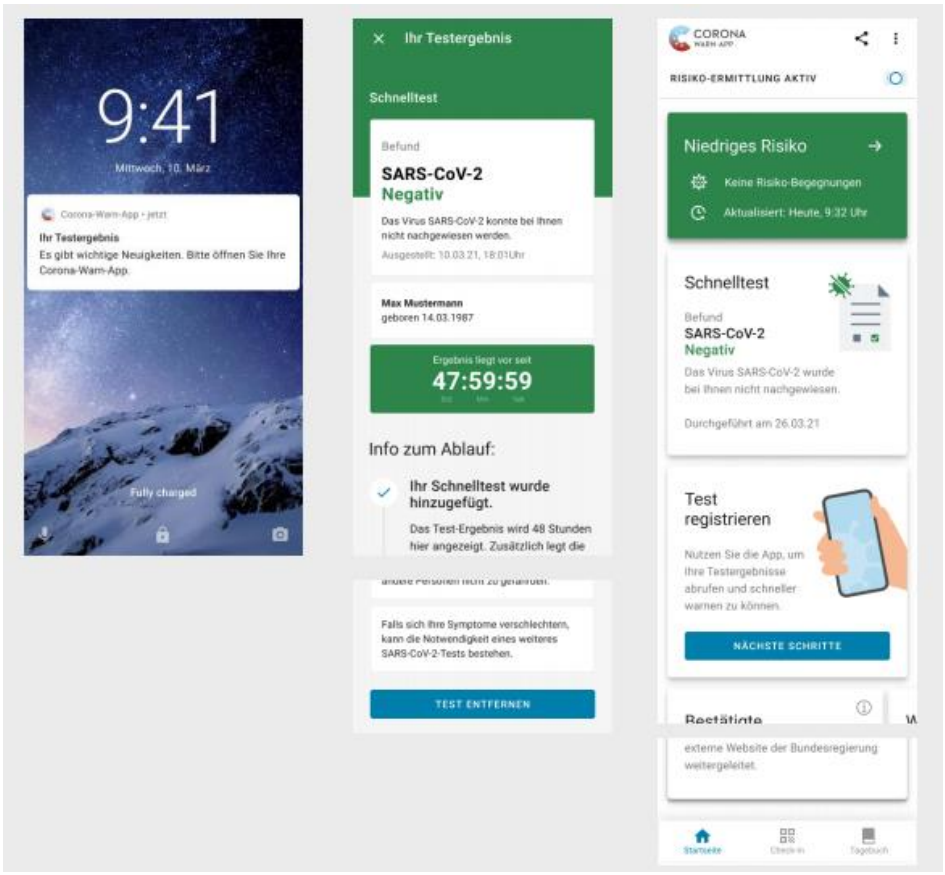

Abbildung 6: Screens in der CWA-App bei negativem Ergebnis (beispielhaft)

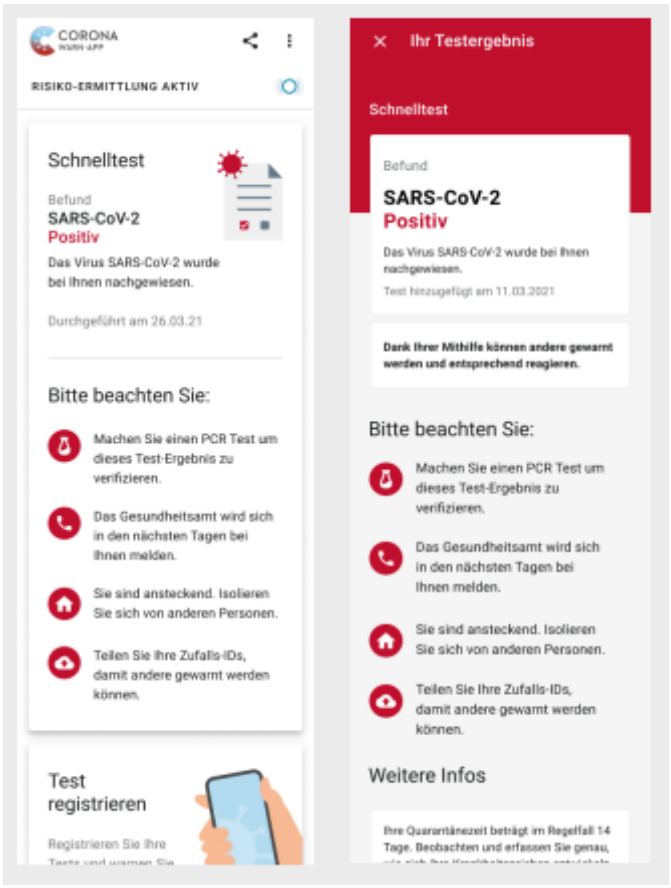

Abbildung 7: Screens in der CWA-App bei positiven Testergebnis (beispielhaft)

Weitere aktuelle Screenshots der App finden Sie hier: https://www.coronawarn.app/de/screenshots/

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.

2.5 Integration des Digital COVID-19 Certificate (DCC)

Dieses Kapitel beschreibt die Anpassungen zur Integration des europäischen digitalen COVID-Zertifikats, auch Digital Covid Certificate (DCC) genannt, im Schnelltest-Portal für Antigentests.

2.5.1 Allgemeine Beschreibung DCC

Das Digital Corona Certificate (DCC) der EU ist ein Nachweis dafür, dass eine Person entweder

- gegen COVID-19 geimpft wurde (COVID-19 Impfzertifikat),
- von COVID-19 genesen ist (COVID-19-Genesenenzertifikat), oder
- mit einem Schnell- oder PCR-Test negativ auf COVID-19 getestet wurde (COVID-19-Testzertifikat)

Für das in diesem Dokument relevante COVID-19-Testzertifikat sieht das Infektionsschutzgesetz vor, dass die Durchführung einer Testung in Bezug auf einen negativen Erregernachweis des Coronavirus SARS-CoV-2 auf Wunsch der getesteten Person durch die zur Durchführung oder Überwachung der Testung berechtigte Person in einem digitalen Zertifikat (COVID-19-Testzertifikat) zu bescheinigen ist (§22 (7) IfSG). Zur Erstellung des COVID-19-Testzertifikats ist laut eben diesem Gesetz die Übermittlung folgender Daten durch die zur Bescheinigung verpflichtete Person an das Robert Koch-Institut erforderlich, das das COVID-19-Testzertifikat hiermit technisch generiert:

1. Name der getesteten Person, Geburtsdatum,
2. Datum der Testung und
3. Weitere Angaben zur Testung, einschließlich der Information über das verwendete Test und zum Aussteller.

Das DCC enthält einen QR-Code mit elektronischer Signatur zum Schutz vor Fälschung. Bei der Kontrolle werden QR-Code und Signatur überprüft. In Deutschland werden zentral Signaturzertifikate (Digital Signer Certificates, DSCs) bereitgestellt, mit denen die ausgestellten DCCs digital unterschrieben werden. Sämtliche Schlüssel werden EU-weit über ein gesichertes Gateway an die Mitgliedsstaaten und von dort an die Apps zur Verifikation (Verifier Apps) weiterverteilt. Hierbei werden keine personenbezogenen Daten des Zertifikat-Inhabers übermittelt, da dies für die Überprüfung der elektronischen Signatur nicht erforderlich ist.

2.5.2 Technische Beschreibung DCC

Um ein DCC, basierend auf einem Antigentest, in der CWA App darstellen zu können, müssen Anpassungen an unterschiedlichen Komponenten vorgenommen werden. Es werden Anpassungen in der CWA App, dem CWA Ecosystem und im Partnerportal erforderlich.

Ziel ist es, ein auf einem Antigentest basierendes DCC, in der CWA App anzuzeigen. Die Übertragung erfolgt verschlüsselt vom Schnelltestzentrum bis zur CWA App.

Ermöglicht wird dies mittels einer Hybridverschlüsselung, für welche die CWA App ein kryptografisches Schlüsselpaar generiert, den privaten Schlüssel geheim hält und den öffentlichen Schlüssel an das CWA Ecosystem weitergibt. Für den Fall, dass ein DCC angefordert wurde, wird der öffentliche Schlüssel an die Teststelle übermittelt. Die Teststelle ermittelt alle für das DCC relevanten Informationen, erstellt einen symmetrischen Schlüssel und verschlüsselt diesen mithilfe des zuvor übermittelten Public Keys. Zudem wird ein Hash der DCC Inhalte erzeugt. Der Hash wird über das CWA Ecosystem signiert und zusammen mit den anderen Daten an die CWA App übertragen. Hier werden nun alle Daten mittels des Private Keys entschlüsselt und das DCC zusammengefügt.

2.5.3 Gesamtablauf CWA mit DCC

Die für die Erstellung und Übermittlung eines digitalen COVID-19-Testzertifikats erforderlichen Komponenten sind die folgenden:

- CWA App: Client Komponente der CWA auf dem Smartphone
- CWA Ecosystem: Gesamtheit aller Server Komponenten, die mit der CWA in Verbindung stehen (Test-Result Server, CWA Verification Server, DCC-Server)
- Issuer Backend: Server Komponente, welche die Signatur erstellt.
- CWA Rapid Test Portal: Software-Lösung für den Schnelltestprozess am Point of Care (PoC)

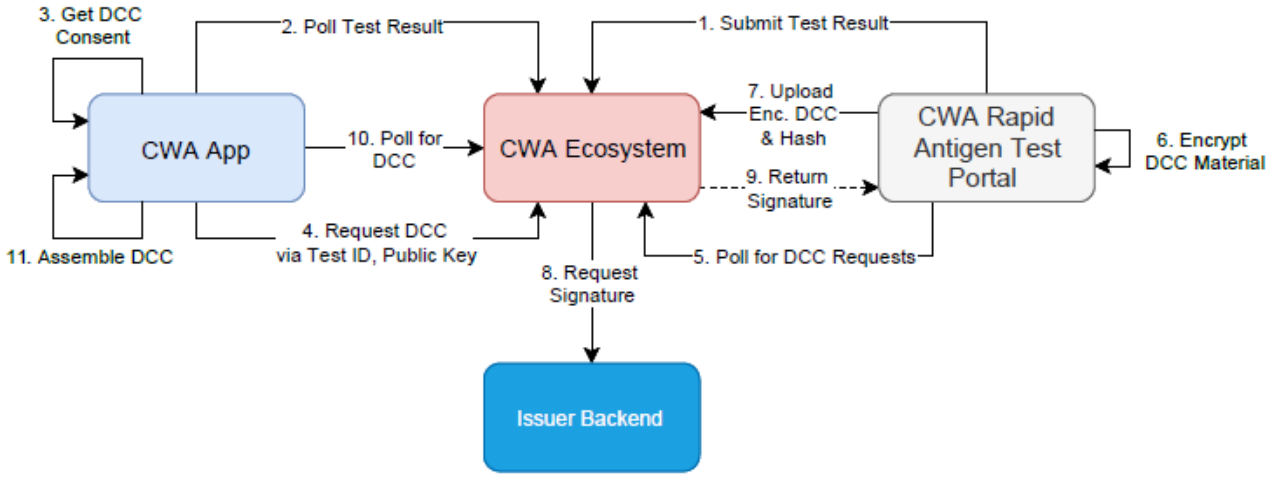

Abbildung 8: Ablauf der einzelnen Prozessschritte ab der Übertragung des Testergebnisses bis zur Erstellung des DCC.

Die Schritte 1 und 2 sind die Abläufe, die bereits im Rahmen des bisherigen Partnervertrags zur Portallösung in der CWA integriert sind. Sie werden bei jedem Antigen Schnelltest in der CWA durchgeführt. Ab Schritt 3 sind die Prozessschritte beschrieben, die zusätzlich für eine Verarbeitung des DCC in der CWA erforderlich sind. Diese Schritte laufen in einer separaten Komponente des CWA Ecosystems, dem CWA DCC Service ab.

1. Submit Test Result
   Sobald ein Testergebnis aus einem Antigen Schnelltest vorliegt, wird das Ergebnis an das CWA Ecosystem (den Test Result Server) übertragen.
2. Poll Test Result
   Das Testergebnis wird von der CWA App per Polling aus dem CWA Ecosystem (dem Verification Server) abgerufen.
3. Get DCC Consent
   In der CWA App wird abgefragt, ob ein DCC benötigt wird.
4. Request DCC
   Die CWA App fragt mittels Test ID und Public Key einen DCC beim DCC Service an.
5. Poll for DCC Requests
   Das CWA Rapid Antigen Test Portal holt sich per Polling die DCC Anfragen vom CWA DCC Service ab.
6. Encrypt DCC Material
   Die DCC Bestandteile werden im CWA Rapid Antigen Test Portal verschlüsselt. Der DCC Payload (Nutzdaten, Bestandteile siehe weiter unten) wird mit einem Data Encryption Key (DEK) verschlüsselt. Der Public Key wird verwendet, um den DEK zu verschlüsseln.
7. Upload enc. DCC and Hash
   Die verschlüsselten DCC Komponenten und der Hashwert werden an das CWA Ecosystem übertragen.
   Im Einzelnen werden in diesem Schritt vom PoC die folgenden Daten übertragen:

   - Test ID
   - Mit DEK verschlüsselter DCC Payload
   - Hash des DCC Payloads
   - Verschlüsselter DEK

8. Reguest Signatur
   Der DCC Service stellt eine Signatur-Anfrage beim Issuer Backend. Das Issuer Backend erstellt die Signatur für den DCC, womit später die Echtheit der Zertifikats überprüft werden kann.
9. Return Signatur
   Die Signatur wird vom DCC Service an das CWA Rapid Antigen Test Portal übertragen.
   Hiermit ist es möglich, dass im CWA Rapid Antigen Test Portal ein DCC inklusive Signatur erstellt werden kann.
   Für die Erzeugung des DCC in der CWA App ist dieser Schritt jedoch nicht notwendig. In Schritt 10 wird die Signatur weiterhin an die CWA App übertragen, was für die Verifikation in der CWA App essenziell ist.
10. Poll for DCC
    Die CWA App holt sich per Polling die DCC Bestandteile (Verschlüsselter DCC Payload, Signaturobjekt und Hash des DCC Payloads) vom DCC Service.
11. Assemble DCC.
    Der DEK wird in der CWA App mit dem Private Key entschlüsselt. Mit dem entschlüsseltem DEK wird in der App der DCC Payload entschlüsselt und gemeinsam mit dem Signaturobjekt zu einem vollständigen DCC zusammengesetzt.

2.5.4 Attribute des DCC Payload

Welche Daten für DCC-Testzertifikate genau zu übertragen sind, wird auf europäischer Ebene in folgender Spezifikation definiert, die bei der Übertragung entsprechend zu befolgen ist.

https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_json_specification_en.pdf

Das DCC Payload enthält die essenziellen Daten des DCCs, welche vom CWA Rapid Antigen Test Portal an das CWA Ecosystem übertragen werden müssen.

Attribut	Beschreibung	Wert / Beispiel
fn	Vorname	Erika
gn	Nachname	Mustermann
fnt	Vorname, maschinenlesbare Form	ERIKA
gnt	Nachname, maschinenlesbare Form	MUSTERMANN
dob	Geburtsdatum	1990-12-23
ci	DCCI	URN:UVCI:V1:DE:DMN3L94E7PBDYYLAPNNSS5T218
sc	Datum / Uhrzeit des Tests	2021-06-01T12:00:00Z
tr	Testergebnis	260415000 (für negativ) 260373001 (für positiv)
tc	Teststelle	FTA Testzentrum
ma	Test Identifier***	1468
	Konstante Werte	
is	Aussteller des Zertifikats	FTA DCC Issuance
ver	Version	1.0.0
co	Das Land des Zertifikatausstellers	DE
tg	Erkrankung, COVID-19	840539006
tt	Typ des Tests, Antigentest	LP217198-3

*** Muss alle 24h auf aktuell zugelassene Tests geprüft werden. Eine Liste mit Tests, die in der EU zugelassen sind ist hier zu finden: https://ec.europa.eu/health/sites/default/files/preparedness_response/docs/covid-19_rat_common-list_en.pdf

3 FUNKTIONSBESCHREIBUNG

Das CWA Schnelltest-Portal in der aktuellen Ausbaustufe umfasst die nachfolgend beschriebenen Funktionen.

Das Schnelltest-Portal wird fortlaufend weiterentwickelt, den gesetzlichen Vorgaben angepasst und ggf. um zusätzliche Funktionen ergänzt. Aktuelle Informationen zur Funktionalität finden Sie hier: https://github.com/corona-warn-app/cwa-quicktest-onboarding/wiki/CWA-Schnelltest-Portal.

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 Funktion 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 Administratoren zugreifen können. Alle nachfolgend beschriebenen Accounts sind diesem Mandanten zugeordnet.

3.1.2 Anlegen und Verwalten von Administratoren

Telekom legt für einen vom Partner benannten Mitarbeiter einen Administrator Account für dessen technischen Mandanten an.

Der Administrator verfügen über die Berechtigung, Benutzer und Teststellen zu verwalten.

Benutzer sind für die Erfassung der Daten der Testperson und für die Eingabe der Testergebnisse zuständig. Für diese Aufgaben sind unterschiedliche Rollen zuständig, die in Kapitel 3.3 beschrieben sind.

Es liegt in der Verantwortung des Partners, dass der Administrator dem Benutzer Zugangsdaten (Nutzername + initiales Passwort) auf einem sicheren Weg mitteilt.

3.1.3 Passwort für Administrator zurücksetzen

Hat ein Administrator sein Passwort vergessen, so kann er es über den Link „Passwort vergessen“ auf der Loginmaske zurücksetzen. Er erhält an die von ihm hinterlegte E-Mail-Adresse einen Link zum Setzen eines neuen Passworts. Beim Setzen des neuen Passworts muss er den Account auch mit einer neue Instanz in seiner OTP-App verknüpfen. Der Passwort-Rücksetzen-Prozess kann also auch genutzt werden, wenn der Administrator keinen Zugriff mehr auf seine OTP-App hat oder sein Smartphone wechselt.

Passwörter von Benutzern kann der Administrator zurücksetzen (siehe 3.2.4)

3.1.4 Anlegen und Verwalten von Benutzern

Der Admin-Bereich des Schnelltest-Portals ermöglicht dem Administrator Accounts für Benutzer anzulegen. Diesen sind nachfolgend die initialen Zugangsdaten (Nutzername + initiales Passwort) auf einem sicheren Weg mitzuteilen.

Der Administrator hat die Berechtigung, die von ihm erstellten Accounts zu ändern und zu löschen.

3.1.5 Anlegen und Verwalten von Teststellen

Die Nutzung des Schnelltestportals erfordert das Anlegen von organisatorischen Teststellen. Eine Teststelle ist zumeist gleichzusetzen mit einer räumlich und/oder organisatorisch abgrenzbaren Schnellteststelle eines Vertragspartners. Mit Teststellen können aber auch z. B. Einsatzschichten oder organisatorische Unterstrukturen abgebildet werden.

3.2 Benutzerverwaltung

Um einen Benutzer verwalten zu können, benötigt der angemeldete User Administrationsrechte. Administratoren müssen vom Betrieb eingerichtet werden. Administratoren sind bestimmten Mandanten zugeordnet und können somit auch nur die Daten des zugeordneten Mandanten bearbeiten. Daten von anderen Mandanten sind nicht einsehbar und somit auch nicht änderbar.

Die Benutzerverwaltung dient dazu die Nutzer des im CWA Antigen Schnelltest Portal innerhalb des eigenen Verantwortungsbereiches zu administrieren. Über den Button „Benutzerverwaltung“ gelangt ein Administrator zur gleichnamigen Eingabemaske. Auf dieser Maske sieht man alle bereits eingegebenen Nutzer und POCs des eigenen Verantwortungsbereiches in Listenform dargestellt. Hier können sowohl Benutzer als auch Teststellen administriert werden.

3.2.1 Benutzer hinzufügen

Über den Button „Neuen Benutzer Hinzufügen“ kommt man auf die Eingabemaske Benutzerdaten.

Auf der Eingabemaske Benutzerdaten können die folgenden Felder gefüllt werden:

- Benutzername (Pflichtfeld)
- Vorname (Pflichtfeld)
- Nachname (Pflichtfeld)
- Passwort (Pflichtfeld)
- Berechtigung für Testerfassung (optionales Feld)
- Berechtigung für Patientendatenerfassung (optionales Feld)
- Teststelle (Pflichtfeld)

Über zwei Checkboxen können dem neuen Benutzer Berechtigungen (siehe Kapitel 2 „Rollen und Rechte“) erteilt werden. Werden keine Berechtigungen zugeordnet, erscheinen für diesen Benutzer im Startbildschirm keine Menüinhalte.

- „Berechtigung für Testerfassung“ (lab): Der Benutzer erhält die Berechtigung, Testergebnisse zu erfassen. Dies ermöglicht ihm Zugang zu den Erfassungsmasken „Testergebnisse eingeben“, „Testergebnisse“ und „Auswertung“.
- „Berechtigung für Patientendatenerfassung“ (counter): Der Benutzer erhält die Berechtigung für die Patientendatenerfassung. Dadurch hat er damit Zugriff auf die Erfassungsmasken „Patientendaten erfassen“ und „QR-Scan erfassen“ und kann Personendaten erfassen.

Einem Benutzer können gleichzeitig mehrere Berechtigungen zugeordnet werden.

Ein neuer Benutzer muss stets auch einer Teststelle zugeordnet werden. Hierbei handelt es sich um ein Pflichtfeld, ohne dessen Auswahl der neue Benutzer nicht gespeichert werden kann. Es ist auch nicht möglich einem Benutzer mehrere Teststellen zuzuordnen.

3.2.2 Benutzer Bearbeiten

Über den Button „Bearbeiten“ kommt man wieder auf die Maske Benutzerdaten. Hier können alle Attribute, wie unter Benutzer anlegen beschrieben, geändert werden.

3.2.3 Benutzer Löschen

Nicht mehr benötigte Nutzer können über den Button „Löschen“ wieder gelöscht werden.

3.2.4 Passwort für Benutzer zurücksetzen

Hat ein Benutzer sein Passwort vergessen, so kann der Administrator in der Eingabemaske „Benutzerdaten“ ein neues Passwort für ihn festlegen.

Die Funktion „Passwort vergessen“ auf der Loginmaske ist nur für Administratoren benutzbar.

Hat der Benutzer keinen Zugriff mehr auf seine OTP-App, z.B. nach einem Gerätewechsel, so kann der Administrator seinen Account löschen und neu anlegen. Beim erneuten Durchlauf des Initialisierungsprozesses ändert der Benutzer dann sein initiales Passwort und verknüpft den Account mit einer neuen Instanz der OTP-App.

3.2.5 Teststelle anlegen

Die Nutzung des Schnelltestportals erfordert das Anlegen von Teststellen. Hier können auch z. B. Einsatzschichten oder organisatorische Unterstrukturen innerhalb einer Teststelle definiert werden.

Da beim Hinzufügen von Benutzern zwingend eine Teststelle zuzuordnen ist, sollte bereits im ersten Schritt mindestens eine Teststelle erstellt werden. Es können beliebig viele Teststellen erstellt werden.

Über den Button „Neue Teststelle hinzufügen“ öffnet sich eine Eingabemaske. Hier geben Sie bitte den Namen und die Adresse der Teststelle an.

- Eingabefeld „Name“ (Pflichtfeld). Bei diesem Feld handelt es sich um ein Freitextfeld. Jeder Name kann nur einmal vergeben werden. Typischerweise wird hier der Name der Teststelle eingetragen. Es gibt weiterhin keinerlei Vorgaben bezüglich des Namens.
- Eingabefeld „Name und Adresse der Teststelle“: Bei diesem Feld handelt es sich um ein Freitextfeld in welches Sie die Daten eingeben, die später auf dem Testbeleg aufgeführt und gedruckt werden, also die formale Bezeichnung der Teststelle und deren Adresse. Sie können falls gewünscht außerdem noch den verantwortlichen Arzt angeben.

  Hinweis: Dieses Feld darf nicht leer sein. Bitte achten Sie bei Ihren Angaben an dieser Stelle auf eine korrekte Eingabe, wie Sie es später auch auf dem Testbeleg abgebildet sehen wollen. Sie können die Eingabe über das Stiftsymbol für die Funktion „Teststelle bearbeiten“ auch nach dem Abspeichern jederzeit korrigieren oder ändern.

- Auswahlkästchen „Im Schnelltestsuchportal anzeigen“. Wird das Kästchen aktiviert, so wird die Teststelle mit der dazugehörigen Adresse im Suchportal unter https://map.schnelltestportal.de/ angezeigt.
  Der Administrator hat die Möglichkeit, optional weitere Informationen zur Teststelle anzeigen zulassen:
  - URL der dazugehörigen Website
  - Öffnungszeiten

- Information, ob eine Terminvereinbarung notwendig ist

3.2.6 Teststelle bearbeiten

Über das Symbol „Bearbeiten“ hinter den in der Benutzerverwaltung aufgelisteten Teststellen können der Name und die Daten für den Testbeleg jederzeit geändert werden. Sie haben außerdem die Möglichkeit, Teststellen hierarchisch zu strukturieren, indem Sie hier eine übergeordnete Teststelle zuweisen.

3.2.7 Teststelle löschen

Über den Button „Löschen“ kann ein nicht mehr benötigte Teststelle gelöscht werden.

Über das Symbol „Löschen“ hinter den in der Benutzerverwaltung aufgelisteten Teststellen können Teststellen aus dem Schnelltestportal gelöscht werden. Es erscheint zunächst der Warnhinweis, ob die Teststelle wirklich gelöscht werden soll. Falls Sie einer Teststelle Untergruppen zugeordnet haben, werden Sie ebenfalls gelöscht. Außerdem verlieren Benutzer Ihre Zugehörigkeit zu dieser Teststelle. Damit diese Benutzer das Schnelltestportal weiterhin einwandfrei nutzen können, müssen die Benutzer einer neuen Teststelle zugeordnet werden.
Eine Teststelle kann nicht gelöscht werden, solange dafür noch offene Tests vorliegen.

3.3 Rollen

Um die verschiedenen Aktivitäten für den Administrationsbereichs bzw. die Benutzerberechtigung durchführen zu können sind verschiedene Berechtigungen notwendig. Diese Berechtigungen werden über Rollen zugewiesen. Hierbei können einer Person mehrere Rollen zugewiesen werden, wodurch sie mehrere Berechtigungen erhält.

Die Administrator Rolle muss von Operations angelegt und einem Testanbieter zugeordnet werden. Der Testanbieter kann selbst Untergruppen entsprechend seiner Teststellen anlegen. Nur mit Hilfe der Rolle Administrator können Benutzer verwaltet werden.

Übersicht der Rollen im System

Nr.	Rolle (Name im System)	Nutzer der Rolle	Beschreibung	Daten	Berechtigung	
					Lesen Read	Schreiben Write[3]
1.	lab / Testerfassung	Testerfassungsnutzer	Benutzer, die Schnelltests erfassen	Setzen des Testergebnisses	X	X
2.	counter / Patientendatenerfassung	Personaldatenerfassungsnutzer	Benutzer, die die persönlichen Daten der zu testenden Personen erfassen	Name, Geburtsdatum, Anschrift	X	X
3.	admin	Administrator	Anlegen von Benutzern und Teststellen. Zuweisung der Rollen und der Teststelle zum Benutzer	Benutzer, Teststelle	X	X

3.4 Login / Zugang

3.4.1 Initial-Login / Aktivierung von Benutzer Accounts

Ein Benutzer- oder Administratoren-Account wird mit der erstmaligen Anmeldung mit dem erhaltenen Benutzernamen und initialen Passwort aktiviert. Nachfolgend muss durch den Benutzer 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 Benutzer 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 Benutzer z.B. eine der nachfolgenden Apps auf seinem Smartphone installieren und verwenden:

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

Zusammenfassend müssen bei der initialen Anmeldung die folgenden Schritte durchlaufen werden:

- Aufruf des Schnelltest-Portals mit dem per E-Mail versandten Link
- Eingabe des Benutzernamens und des initialen Passworts
- Ersetzen des initialen Passworts durch ein persönliches Passwort.
  Auf der Folgemaske wird ein QR-Code angezeigt
- Scannen des QR-Codes mit einer 2FA-App, daraufhin wird ein Einmalpasswort in der App angezeigt (das Scannen des QR-Codes ist nur bei der Erstanmeldung relevant)
- Eingabe des 6-stelligen Einmalpasswortes in der Anmeldemaske

3.4.2 Benutzer-Login (mit Zwei-Faktor-Authentisierung)

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

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

Auf der Login-Seite (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 Benutzernamen und der Zeitangabe gespeichert.

Zusammenfassend müssen bei der 2. Anmeldungen die folgenden Schritte durchgeführt werden:

- Aufruf des Schnelltest-Portals
- Eingabe des Benutzernamens und des persönlichen Passworts
- Öffnen der 2FA-App und auslesen des Einmalpasswortes
- Eingabe des Einmalpasswortes in der Anmeldemaske

3.4.3 Benutzer-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 Benutzer zur Verantwortung gezogen werden.

3.5 Erfassung der persönlichen 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.

3.5.1 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 Benutzer 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. Über ein Freitextfeld können zusätzliche Informationen (z.B. die Nummer des Personalausweises) eingegeben werden, die auf dem Testbeleg anzeigt werden sollen.

Im Zusammenhang mit der Datenerfassung und -verarbeitung wird auf der Erfassungsmaske über zwei Radiobuttons (siehe Punkt 1 und 2 unten) das Einverständnis des Patienten für die Übertragung seines Testergebnisses in die CWA (Fall 1 anonym, Fall 2 Ergebnis mit Name, Vorname, Geburtsdatum) 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 Name und Geburtsdatum an die App zur Anzeige des Testergebnisses in der App als namentlicher Testnachweis ein. Dem Getesteten wurden Hinweise zum Datenschutz ausgehändigt.“

Wurde keine der beiden Optionen ausgewählt, erfolgt keine Übertragung von Daten in die CWA. Wurde versehentlich einer der Radiobuttons angeklickt, so kann dieser durch erneutes Anklicken deaktiviert werden.

Außerdem wird in einer Checkbox der Wunsch des Patienten nach einer Dokumentation des Ergebnisses als DCC abgefragt:

3) **Bestätigung, dass ein DCC gewünscht ist**
   Über die Checkbox mit der Beschriftung "Der Patient wünscht ein offizielles COVID-Testzertifikat der EU (DCC)." wird dokumentiert , dass ein DCC gewünscht ist, es werden mehrere Prozessschritte in Kraft gesetzt.
   1. Auf der Eingabemaske erscheinen die Felder „Standardisierter Vorname“ und „Standardisierter Name“. Für den weiteren Ablauf müssen beide Felder zwingend befüllt werden.
   2. In der Maske Datenerfassung können in der Dropdown-Liste „Testhersteller und -name“ nur noch Tests ausgewählt werden, die DCC-konform sind. Es handelt sich hierbei um eine EU-weit anerkannte Liste von Antigen-Schnelltests.
   3. Im gespeicherten Datensatz wird das Flag „DCC=True“ gesetzt
   4. Nur wenn die drei vorausgegangenen Schritte beachtet wurden, kann später nach Vorliegen des Testergebnisses in der CWA App ein DCC angefordert werden.

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

3.5.2 Scannen eines QR-Codes (vCard) der Testperson

Hinweis: der unten beschriebene Prozess setzt voraus, dass das Schnelltestportal auf einen Gerät (Tablet, Smartphone) mit integrierter Kamera genutzt wird

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 Benutzer auf der Startseite des CWA Schnelltest-Portals die Funktion „QR-Code scannen“ und scannt den durch die Testperson überderen Smartphone vorgelegten QR-Code mit der Kamera seines Gerät.

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 3.5.1 beschriebenen Vorgehensweisen zur Aushändigung von Datenschutzhinweisen und Einwilligungen vorzunehmen.

Bei einer Zustimmung, dass der Patient einen DCC wünscht, werden die gleichen Mechanismen in Kraft gesetzt, wie sie bereits in Kapitel 3.5.1 unter Punkt 3 beschrieben sind.

3.6 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 Probenidentifier (Proben-ID). Die Proben-ID wird am rechten oberen Rand der Erfassungsmaske automatisch angezeigt und wird weiterhin für die spätere Eingabe des Testergebnisses sowie des Auswahl und Anzeige von Testbelegen benötig. Die Proben-ID ist vom Benutzer im Testprozess händisch auf den Test zu übertragen.

Die Proben-ID setzt sich aus den ersten 8 Stellen der im Schnelltest-Portal Backend erstellten CWA Test ID zusammen. (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.

3.7 Speichern des Datensatzes

3.7.1 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 Benutzer 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 Infrastuktur) „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	tbd	Test-ID des verwendeten Tests Handelsname (nach BfArM Liste zugelassener Antigentests: https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/Spezialthemen/Antigentests/_node.html)
test_brand_name	text	Antigentest Handelsname (nach BfArM Liste zugelassener Antigentests: https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/Spezialthemen/Antigentests/_node.html)
salt	text	Generierte 128-Bit Zufallszahl in Hexadezimal-Darstellung, nur mit Großbuchstaben und fester Breite von 32 Stellen**
test_sample-ID	text (8)	Die ersten 8 Zeichen der hash(CWA Test-ID) Proben-ID “67a50cba”
test_time	unix timestamp, seconds	Test Datum und Uhrzeit werden auf auf dem PoC-Backend gesetzt, um Manipulationen zu verhindern
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 generierte Zeichenkette empfohlen. Anstelle der UUID Typ 4 kann vom Partner auch eine eigene Test-ID verwendet werde, diese ist in JSON als Zeichenkette zu behandeln.
CWA_Test-ID	Text	SHA256-Hashwert aus den JSON-Objekten `[dob] # [fn] # [ln] # [timestamp] # [internal-id] # [salt]`
Hash(CWA_Test-ID)	Text	Ist die gehashte CWA_Test-ID, die noch ein zweitesmal mit SHA256 gehasht wurde (Doppel Hashing). Dies ist notwendig, um den selben Ablauf beim Test Result Server verwenden zu können, so wie er von den Laboren angewendet wird

Des Weiteren werden folgende Daten im Administrationsbereich verarbeitet und gespeichert:

Attribute	Type	Kommentar
	Mandant	
mandant-ID	tbd	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	tbd	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 die Tests der Teststelle „Sabine“
poc_responsible_last_name	text	Verantwortlicher für die Tests der Teststelle „Dr. Musterfrau“

Für das DCC werden zusätzlich die folgenden Attribute gespeichert.

Attribute	Type	Kommentar
	quick_test	
standardised_family_name	text	„MUSTERMANN“
standardised_given_name	text	„MAX“
disease_agent_targeted	text	„COVID-19“
dcc_consent	text	User wünscht ein DCC (ja/nein)
dcc	text	Das signierte DCC
dcc_unsigned	text	Das unsignierte DCC
dcc_status	int	Aktueller Status des DCC, während des Prozesses
dcc_public_key	text	Public Key für die End-to-End Verschlüsselung
dcc_sign_data	text	Signierungsdaten

3.7.2 Archivierung / Speicherung der Testergebnisse

Auf dem Schnelltest-Portal Backend sind die Daten des Testvorgangs (Daten des Probanden, Daten zur Durchführung des Tests und Testergebnisse) 14 Tage für die Benutzer des entsprechenden Mandanten (Administratoren, Erfasser von Probandendaten und Erfasser von Testergebnissen des Partners), der den Test durchgeführt hat, abrufbar.

Nach Ablauf der 14 Tage werden die Daten automatisiert verschlüsselt und in einem Langzeitarchiv abgelegt, das aus rechtlichen Gründen die Daten für 10 Jahre speichert. T-Systems ist berechtigt, dem Partner die Daten aus dem Langzeitarchiv einmalig zur Gänze zum Abruf in angemessener Form zur Verfügung zu stellen, insbesondere zum Ende der Vertragslaufzeit. Hierdurch sind sämtliche Ansprüche des Partners auf Zugriff auf das Langzeitarchiv erfüllt und T-Systems ist berechtigt, das Langzeitarchiv des Partners zu löschen.

Darüber hinaus steht Partner kein Anspruch auf Zugriff auf das Langzeitarchiv zu.

T-Systems ist berechtigt und verpflichtet, die Daten aus dem Schnelltest-Portal Backend zum Ende des Vertrags dauerhaft zu löschen. Eine weitere Herausgabe von Daten erfolgt nicht.

3.7.3 Funktion zur Ermittlung des Testzeitpunkts

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

3.7.4 Returncodes zur Mitteilung der erfolgreichen Speicherung des Datensatzes

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

3.8 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 Benutzeroberfläche 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.

3.9 Erfassen des Testergebnisses

Nach Durchführung eines Schnelltests können die Benutzer in der Teststelle über das Hauptmenü die Funktion „Testergebnis erfassen“ anwählen und in einer entsprechenden Eingabemaske das Testergebnis zu einem Testvorgang eingeben. Um die hier beschriebenen Prozessschritte durchführen zu können ist zu können benötigt der Benutzer die Rolle lab (siehe hierzu auch Kapitel 3.3)

3.9.1 Eingabe des Probenidentifiers (Proben-ID)

Um den Test eindeutig einem Vorgang und damit einer Testperson zuordnen zu können, wird die bei der Erfassung der personenbezogenen Daten automatisch vergebene Proben-ID (siehe 3.6 Probenidentifikation) verwendet. Diese sollte zudem auf der Probe selbst vermerkt werden.

Nach Aufruf der Funktion „Testergebnis erfassen“ wird zunächst ein PopUp-Fenster angezeigt, in dem die Proben-ID abgefragt wird Anhand der Proben-ID wird im Backend überprüft, ob der Patient ein DCC angefordert hat. Wenn nein, verläuft der Prozess wie in 3.9.2 beschrieben. Wenn ja, verläuft der Prozess wie in 3.9.3 beschrieben. Dem Tester werden in der darauffolgenden Maske, in einer DropDown-Liste für das verwendete Testmaterial nur Test-Kits aus der von der EU freigegebenen Liste zur Auswahl angeboten (EU RAT-Liste).
Im Nicht-DCC-Fall kann der Tester aus der Liste der Bundesanstalt für Arzneimittel und Medizinprodukte (BfArM) auswählen.

3.9.2 Ablauf im Nicht-DCC-Fall

Ist in der Eingabemaske zur Erfassung der persönlichen Daten (siehe Kapitel 3.5) auf die Ausstellung eines DCC verzichtet worden, werden in der Erfassungsmaske des Testergebnisses zwei Eingabefelder für die Bestimmung des verwendeten Tests angezeigt. Der Tester hat die Auswahl, ob er die Test-ID eingeben möchte oder den Handelsnamen. Das jeweils andere Feld wird automatisch im Hintergrund befüllt.

3.9.2.1 Eingabe der Test-ID

Um den Anforderungen an die Erstellung eines einfachen Testbelegs (ohne DCC) 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. Über eine Auswahlliste aller zugelassenen Test kann die Test-ID ausgewählt werden. Nach der Auswahl erfolgt automatisch die Anzeige des Handelsnamen des Herstellers und die Befüllung des dazugehörigen Felds.

3.9.2.2 Eingabe des Handelsnamens eines Tests

Um den Anforderungen an die Erstellung eines Testnachweises und der Meldung im Positiv-Fall zu genügen ist in weiterhin der Handelsname des verwendeten Test-Typs (gemäß BfArM Liste zugelassener Antigentests) einzugeben. Über eine Auswahlliste kann der Handelsnamen des Herstellers ausgewählt werden. Nach der Auswahl erfolgt gleichzeitig die Anzeige der Test-ID und die Befüllung des dazugehörigen Felds.

3.9.3 Ablauf im DCC-Fall

Wurde in der Eingabemaske zur Erfassung der persönlichen Daten (siehe Kapitel 3.5) die Ausstellung eines DCC ausgewählt, wird in der Erfassungsmaske des Testergebnisses nur ein Eingabefeld für die Bestimmung des verwendeten Test angezeigt. Der Tester wählt in diesem aus einer DropDown-Liste, die ausschließlich die von der EU freigegebenen Test-Kits (EU RAT-Liste) enthält, einen Eintrag für Testhersteller und -name aus.

3.9.4 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.

3.10 Persistieren des Testergebnisses

3.10.1 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.

3.10.2 Persistieren des Testergebnisses in der Datenbank

Wird zu einem angelegten Datensatz mit Name, 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 automatisiert verschlüsselt und in einem Langzeitarchiv abgelegt, das aus rechtlichen Gründen die Daten für 10 Jahre speichert. T-Systems ist berechtigt, dem Partner die Daten aus dem Langzeitarchiv einmalig zur Gänze zum Abruf in angemessener Form zur Verfügung zu stellen, insbesondere zum Ende der Vertragslaufzeit. Hierdurch sind sämtliche Ansprüche des Partners auf Zugriff auf das Langzeitarchiv erfüllt und T-Systems ist berechtigt, das Langzeitarchiv des Partners zu löschen.

Darüber hinaus steht Partner kein Anspruch auf Zugriff auf das Langzeitarchiv zu.

T-Systems ist berechtigt und verpflichtet, die Daten aus dem Schnelltest-Portal Backend zum Ende des Vertrags dauerhaft zu löschen. Eine weitere Herausgabe von Daten erfolgt nicht.

3.11 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.

3.11.1 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 personenbezogene Weiterleitung zugestimmt wurde. Die personenbezogenen Daten werden nicht über das CWA Ecosystem übermittelt, sondern über den QR-Code, den der Benutzer mit der CWA einscannt.

3.11.2 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.

3.12 Infektionsmeldung an das zuständige Gesundheitsamt (Positiv-Meldung)

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

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

3.12.1 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.

3.12.2 Auswahl positiver Testergebnisse

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

3.12.3 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.

3.12.4 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 solchen Ausdrucks liegt in der Verantwortung des Teststellenbetreibers.

3.12.5 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 einem solchen Ausdruck liegt in der Verantwortung des Teststellenbetreibers.

3.13 Testdokumentation / KV-Abrechnung

Das Schnelltest-Portal unterstützt die Abrechnung eines Teststellenbetreibers gegenüber den zuständigen KV 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.

3.13.1 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 ausschließlich für den jeweiligen Tag, 00:00 bis 24.Uhr). Eine nachträgliche Anzeige für vorhergehende Tage ist nicht verfügbar.

3.14 Anzeige, Druck und Download von Testnachweisen ohne DCC

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

3.14.1 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 Benutzer des entsprechenden Mandanten, der den Test durchgeführt hat, abrufbar.

3.14.2 Auswahl eines Testnachweises

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

3.14.3 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.

3.14.4 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 solchen Ausdrucks liegt in der Verantwortung des Teststellenbetreibers.

3.14.5 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 einem solchen Speicherung liegt in der Verantwortung des Teststellenbetreibers.

3.15 Anzeige, Druck und Download von DCC Testzertifikaten

Voraussetzung für die Erstellung eines DCC ist, das die Testperson hierfür zunächst ihre Zustimmung gegeben hat. Dies wird durch die Auswahl des Menüpunkts „Patientendaten erfassen“ auf der Maske Datenerfassung dokumentiert.

Mit der Bestätigung „Patient wünscht ein offizielles COVID-Testzertifikat der EU (DCC)“ werden weitere Eingabefelder angezeigt und die Auswahl der Testkits auf DCC konforme Testkits eingeschränkt.

Weiterhin ist notwendig, dass die Testperson einwilligt, dass das Testergebnis in der CWA angezeigt werden kann. Dies erfolgt über eine Auswahl auf der gleichen Maske. Ein entsprechender Hinweistext wird auf der Maske Datenerfassung angezeigt. Sollte der Patient der Übertragung in die CWA nicht zugestimmt haben, kann aktuell auch kein Testbeleg mit DCC ausgestellt werden.

Nachdem die Testperson ein negatives Testergebnis im CWA Client angezeigt bekommt, kann im CWA Client auf dem Endgerät der Testperson ein DCC angefordert werden. Der technische Ablauf, der hierbei in Kraft gesetzt wird ist in Kapitel 2.5 Integration des Digital COVID-19 Certificate (DCC) beschrieben.

Unter dem Menüpunkt Testergebnisse kann das Testergebnis angezeigt werden. Sollte zuvor im CWA Client auf dem Endgerät der Testperson ein DCC angefordert worden sein, so wird neben dem Testergebnis zusätzlich das DCC dargestellt.

Über das Drucken Symbol, auf der Maske Testergebnisse, wird dann das Testergebnis und zusätzlich der DCC ausgedruckt.

3.16 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 Benutzers und Mandanten bei Hochladen eines Ergebnisses

Die Logging-Daten werden im Backend für 4 Wochen gespeichert und dann gelöscht.

3.17 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 Ecosystem (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, als auch die Plattform zur Übertragung der Testergebnisse an die Corona Warn App. 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:

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

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

Ein Ausfall bedeutet, dass der Anwendungsfalls Transport 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:

1 Ausfälle aufgrund von erforderlichen Wartungsarbeiten
2 Ausfälle aufgrund von Störungen auf Infrastrukturebene Auftraggeber-seitig oder Zulieferern des AG
3 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:

i. exklusive Support Rufnummer (+49 620 2274 3730) für alle Partner mit unterschriebenem Partnervertrag.
ii. First Level Support mit Annahme der Problem-Meldung, Analyse und ggfs. sofortige Lösung.
iii. 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.
iv. 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.

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 von Montag bis Sonntag von 06.00 bis 20.00 Uhr abgefragt, soweit diese Tage keine bundeseinheitlichen 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 oder bis zur Wiederherstellung.

	Kritisch (Prio 1)	Schwer (Prio 2)	Leicht (Prio 3)
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 zur 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

Telekom stellt für den Partner ein Portal zur Erstellung des Mandanten-Admin-Zugangs bereit. Der Partner nutzt dieses Portal, um einen eigenen Mandanten-Admin-Zugang zu erstellen. Der Partner ist verpflichtet, die Zugangsdaten, die er für die eigenen Mandanten-Admin-Zugänge erstellt, geheim zu halten und ist für die Sicherheit dieser Zugangsdaten verantwortlich.

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. Partner ist für die Sicherheit dieser Zugangsdaten verantwortlich.

Erkennt Partner eine unberechtigte Nutzung von Zugangsdaten des Partners, ist er verpflichtet, Telekom die unberechtigte Nutzung unverzüglich anzuzeigen und die Zugangsdaten mittels des von Telekom bereitgestellten Portals zu ändern.

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 Nutzername + 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:

1. FreeOTP
2. Google Authenticator
3. Microsoft Authenticator

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

5.4 Allgemeine Mitwirkungspflichten

5.4.1 Ansprechpartner

Der Partner ist verpflichtet, einen oder mehrere qualifizierte und entscheidungsbefugte Ansprechpartner zu benennen und deren Erreichbarkeit/Vertretung während der Vertragslaufzeit sicherzustellen. Die Ansprechpartner können unterschiedliche Qualifikationen und Entscheidungsbefugnisse aufweisen, Partner stellt jedoch sicher, dass die für den Betrieb erforderlichen Entscheidungen getroffen werden können.

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 Leistungserbringung wesentliche Informationen, d.h. Informationen zu Änderungen der Leistungen und der rechtlichen Bedingungen, sowie Rechnungen ausschließlich per Mail versendet 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 branchenspezifischen 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 missbräuchliche Nutzung liegt insbesondere vor, wenn die Leistungen von Unbefugten verwendet werden, 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 missbräuchlichen 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 unberechtigtem 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 unberechtigtem 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
CWA Ecosys-tem	CWA Ecosystem: Gesamtheit aller Server Komponenten, die mit der CWA in Verbindung stehen (Test Result Server, Verification Server, DCC Server)
ENF	Exposure Notification Framework
GUID	Globally Unique Identifier
LIS	Laboratory Information System

PoC	Point of Care
OTC	Open Telekom Cloud
QR-Code	Quick Response Code
UUID	Universally Unique Identifier