

CORONA

WARN-APP

EXTERNAL

Anlage 1 zum DSFA-Bericht:

c.) Designentscheidungen bei der Entwicklung der Antigen-Schnelltest-Anbindung an die Corona-Warn-App der Bundesrepublik Deutschland und Nachweisfunktion

Ergänzende Dokumentation zum Release 2.5 (Stand: 09.07.2021)

A. Vorwort

Mit diesem Dokument soll für die Öffentlichkeit nachvollziehbar dargestellt werden, welche Designentscheidungen getroffen wurden, um die Antigen-Schnelltest-Anbindung an die Corona-Warn-App und die Anzeigefunktion grundrechtsschonend auszugestalten. Die Funktion wurde mit Release 2.1 implementiert. Das Schnelltest-Profil wurde mit Release 2.2 implementiert. Des Weiteren sind im vorliegenden Dokument die Designentscheidungen im Zusammenhang mit der Umsetzung der Wallet-Funktion der CWA für Impf-, Test- und Genesenzertifikate dargelegt, wie sie in den Releases 2.3, 2.4 und 2.5 umgesetzt wurden.

Das vorliegende Dokument ergänzt folgendes bestehendes Dokument:

Die „Designentscheidungen bei der Entwicklung der Corona-Warn-App der Bundesrepublik Deutschland“ [Anlage 1_2021_2004 a.) Designentscheidungen_CWA_v2.4_Änderungsfassung – im Folgenden auch „Designentscheidungen a.)“], die initial zum GoLive (15.06.2020) erstellt und im Releasezyklus der CWA aktualisiert wurden. Diese gelten zusätzlich. Mit der Dokumentation in einem separaten Dokument soll dem Umstand Rechnung getragen werden, dass eine Zweckerweiterung erfolgt, die ursprünglich nicht Gegenstand der Betrachtungen war.

Wie generell bei der Entwicklung der Corona-Warn-App, wird der Datenschutz ganzheitlich, integrativ und kreativ in den Technologien, Abläufen und Informationsarchitekturen eingebettet werden. Ganzheitlich, weil zusätzliche, breitere Zusammenhänge und Akteure (u.a. Antigen-Schnelltest-Anbieter, Schnittstellen) berücksichtigt werden müssen. Integrativ, weil alle Beteiligten und Interessen konsultiert werden sollten. Kreativ, weil die Einbettung des Datenschutzes bedeutet, bestehende Entscheidungen neu zu erfinden, weil die Alternativen inakzeptabel sind. Das Ergebnis ist, dass der Datenschutz zu einem wesentlichen Bestandteil der bereitgestellten Kernfunktionalität der CWA, aber auch der zusätzlichen Funktionalität der Antigen-Schnelltest-Anbindung wird. Der Datenschutz ist integraler Bestandteil des Systems, ohne die Funktionalität zu beeinträchtigen. Zur Erreichung dieser Ziele und Vermeidung von Risiken für den Datenschutz wurden bei der Entwicklung der Antigen-Schnelltestanbindung an die Corona-Warn-App und ihre Infrastruktur die in diesem Dokument aufgeführten Designentscheidungen getroffen. Die Entwicklung ist zum Zeitpunkt der Erstellung des Dokuments noch nicht abgeschlossen und wird aktualisiert und ergänzt.

In diesem Dokument wird – ausschließlich zum Zweck der besseren Lesbarkeit – auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen in diesem Dokument sind somit geschlechtsneutral zu verstehen.

B. Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	CWA Version			
1	21.04.2021	2.1	Finale Version 1.0		final
2	02.05.2021	2.1	Anpassungen in D-2.1-3, 2.3-1, D-3.1-1, D-4-4		final
3	06.05.2021	2.2	Ergänzungen Schnelltest-Profil in D-2-3, D-9-5a		final
4	20.05.2021	2.3	Ergänzungen Anzeige Impfzertifikate in D-2-4, D-9-5b		final
5	10.06.2021	2.4	Ergänzungen Erstellung/ Anforderung/ Anzeige Testzertifikate in D-2-5, D-2.1-3, D-4-2, D-4-4, 5-1-8, D-9-5c		final
6	01.07.2021	2.5	Anpassung D-9-5c (Löschung auf DCC-Server nach Abstimmung), Ergänzungen Anzeige Genesenenzertifikate in D-2-6, D-9-5d sowie Funktion für Familienzertifikate in D-2-7, D-9-5e		offen

C. Inhaltsverzeichnis

A. Vorwort	2
B. Änderungshistorie	3
C. Inhaltsverzeichnis	4
D. Quellenverzeichnis	6
E. Ziele des Dokuments	7
F. Beschreibung der Funktion Antigen-Schnelltest-Anbindung für die Corona-Warn-App, Schnelltestprofil, Anzeige von Impf-, Test- und Genesenzertifikaten sowie der Funktion für Familienzertifikate.....	8
A. Allgemein.....	8
B. Point-of-Care (PoC): Portallösung und Antigen-Schnelltest-Schnittstelle für Drittanbieter.....	9
C. Testregistrierung: Übertragung von Antigen-Schnelltestergebnissen in die CWA.....	9
C.1. Pseudonymisierte Übermittlung des Antigen-Schnelltestergebnisses.....	9
C.2. Personalisierte Übermittlung des Antigen-Schnelltestergebnisses.....	10
B.3. Anzeige von Schnelltestergebnissen in der CWA – App	10
B.4 Warnung auslösen.....	10
D. Digitale COVID-Zertifikate: Verwalten der Zertifikate in der CWA.....	11
G. Designentscheidungen	13
I. Bedrohungen für den Datenschutz.....	13
1. Zweckgebundenheit & Epidemiologischer Sinn	13
2. Zweckerfüllende Funktionalität der App	16
2.1 Fehlfunktion.....	25
2.2 Fehlgebrauch	27

2.3	Vertrauensverlust der Bevölkerung in Vertrauenswürdigkeit der App	28
3.	Rechtmäßigkeit der Verarbeitung	29
3.1	Freiwilligkeit der Nutzung der CWA-App / der Schnelltestanzeige und der digitalen Nachweisfunktion und der Einwilligungen in die Datenverarbeitung	29
3.2	Freiheitsbeschränkungen bei Nichtnutzung der Nachweisfunktion oder Freiheitsgewinne bei Nutzung der Nachweisfunktion /erzwungene Einwilligung.....	33
3.3	Gefahr der Diskriminierung	34
4.	Transparenz	35
5.	Verdecktheit/ Unbeobachtbarkeit und Vertraulichkeit.....	38
5.1	Anonymität/Pseudonymität und verschlüsselte Speicherung der Pseudonyme.....	38
5.2	Grundlegende Privatsphäre.....	44
6.	Datensparsamkeit/ Datenminimierung	46
7.	Zweckbindung/ Nichtverkettbarkeit.....	48
8.	Intervenierbarkeit.....	49
9.	Löschung/ Speicherbegrenzung.....	51
10.	Trennungskontrolle	56
11.	Vertragsverhältnisse	60
II.	Bedrohungen durch Hacker, Trolle, Stalker und Einzelpersonen (STRIDE)	63
1.	Spoofing (Identität verschleiern)	64
2.	Tampering (Daten verändern)	65
3.	Repudiation (Abstreiten) - keine Besonderheiten für PoC-Anbindung und Nachweisfunktion	65
4.	Information Disclosure (Datenleck) - keine Besonderheiten für PoC-Anbindung und Nachweisfunktion	65
5.	Denial of Service (Mutwillige Überlastung) – keine Besonderheiten für PoC-Anbindung und Nachweisfunktion.....	65
6.	Elevation of Privilege (Ausweiten der Rechte) - keine Besonderheiten für PoC-Anbindung und Nachweisfunktion.....	65

D. Quellenverzeichnis

Bei den ergänzenden Designentscheidungen der Antigen-Schnelltest-Anbindung an die Corona-Warn-App (CWA) der Bundesregierung Deutschland wurde für die hier gemachten Angaben insbesondere auf folgende (öffentliche) Dokumente zurückgegriffen:

- Dokumentationen zu den einzelnen Komponenten der CWA App, zu finden auf den Websites von github.com zur CWA App. Die Dokumentationen auf github.com, die auf Englisch vorliegen, werden regelmäßig aktualisiert und sind den deutschen Übersetzungen in Hinblick auf die Aktualität deshalb vorzuziehen:
 - T/SAP Dokumentation, Scoping Document¹
 - T/SAP Dokumentation, CWA User Interface Screens²
 - T/SAP Dokumentation, Solution Architecture³
 - T/SAP Dokumentation, Sicherheit⁴
 - T/SAP Dokumentation, CWA Verification Server⁵
 - T/SAP Dokumentation, Software Design Verification Server⁶
 - T/SAP Dokumentation, CWA App⁷
 - T/SAP Dokumentation, CWA Server⁸
 - T/SAP Dokumentation, CWA Portal Server⁹
 - T/SAP Dokumentation, CWA Test Result Server¹⁰

¹ https://github.com/corona-warn-app/cwa-documentation/blob/master/scoping_document.md

² https://github.com/corona-warn-app/cwa-documentation/blob/master/ui_screens.md

³ https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md

⁴ <https://github.com/corona-warn-app/cwa-documentation/blob/master/overview-security.md>

⁵ <https://github.com/corona-warn-app/cwa-verification-server>

⁶ <https://github.com/corona-warn-app/cwa-verification-server/blob/master/docs/architecture-overview.md>

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

⁸ <https://github.com/corona-warn-app/cwa-server>

⁹ <https://github.com/corona-warn-app/cwa-verification-portal/blob/master/README.md>

¹⁰ <https://github.com/corona-warn-app/cwa-testresult-server/blob/master/README.md>

E. Ziele des Dokuments

Zur laufenden Verbesserung und Berücksichtigung der Datenschutzanforderungen wurde während des gesamten Entwicklungsverlaufs der Corona-Warn-App eine Datenschutzfolgenabschätzung (DSFA) durchgeführt, auch für die Antigen-Schnelltestanbindung.

Eine DSFA ist eine Risikoanalyse und -bewertung für die Verarbeitung personenbezogener Daten. Es wird abgeschätzt, welche Gefährdungen für die Rechte und Freiheiten natürlicher Personen durch die Datenverarbeitungen bestehen und wie wahrscheinlich es ist, dass diese Gefährdungen eintreten. Die Erkenntnisse aus der ständig begleitenden DSFA sind in den Entwicklungsprozess als Designentscheidungen eingeflossen.

Inhaltlich wurde bei der DSFA die Perspektive des von der Datenverarbeitung Betroffenen – also in der Regel der CWA-Nutzer, daneben aber auch andere Nutzer und Kontaktpersonen des CWA-Nutzers – in den Fokus der Risikobetrachtungen genommen. Damit wurde einer Grundanforderung Rechnung getragen, die auch der „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.“ (FifF) in seiner Datenschutzfolgenabschätzung¹¹ formuliert. Insbesondere wurden Risiken für immaterielle Schäden der Benutzer betrachtet, also drohende gesellschaftliche und soziale Nachteile, Diskriminierungen, Einschüchterungseffekte und die (selbstaufgelegte) Einschränkung von Grundrechten. Weiterführende Informationen finden sich in dem ausführlichen Bericht zur Datenschutzfolgenabschätzung für die Corona-Warn-App sowie den weiteren Anlagen zum Bericht (Anlage 2: Technische und Organisatorische Maßnahmen sowie die Anlagen 3–8 Risikomatrizen für die einzelnen Verarbeitungstätigkeiten).

Dieses Dokument soll der datenschutzinteressierten Öffentlichkeit dazu dienen, anhand der aufgeführten Anforderungen zu prüfen und zu bewerten, inwieweit ein grundrechtsschonendes Privacy by Design auch für die Funktionen gelungen ist, die durch eine ausdrückliche Zweckerweiterung der App erfolgen und damit die Transparenz fördern. Anregungen und Kritik sind ausdrücklich erwünscht, um die Prozesse weiter zu verbessern.

¹¹ FifF DSFA, S. 11. Die Kritik des FifF an der CWA-DSFA [Link: https://www.fiff.de/dsfa-corona-kritik/at_download/file (zuletzt aufgerufen am 12.06.2021)] wurde ebenfalls analysiert und bei der Fortführung der DSFA insbesondere dadurch berücksichtigt, dass die durch Service Provider (Telekom, SAP, Apple und Google) weiterhin ausgewiesen und kontinuierlich betrachtet wurden. Methodisch wird die DSFA laufend verbessert, wobei der Focus weiterhin darauf liegt, Risiken bereits in der Entwicklungsphase zu erkennen und ihnen zu begegnen.

F. Beschreibung der Funktion Antigen-Schnelltest-Anbindung für die Corona-Warn-App, Schnelltestprofil, Anzeige von Impf-, Test- und Genesenzertifikaten sowie der Funktion für Familienzertifikate

Mit Version 2.1 wird es ermöglicht, mit Einwilligung der CWA-Nutzer Corona-Schnelltestergebnisse in die CWA zu übertragen, die digitale Anzeige des Infektionsstatus in der CWA-App zu ermöglichen und – im Falle eines positiven Schnelltestergebnisses – Kontakte zu warnen. Damit soll – analog zur bisherigen Vorgehensweise bei PCR-Tests, die frühe Unterbrechung von Infektionsketten unterstützt werden.

Zur besseren Lesbarkeit des Dokumentes wird an dieser Stelle kurz auf die allgemeine Funktion der CWA eingegangen und danach werden die Antigen-Schnelltest-Anbindung an die Corona-Warn-App, das Schnelltestprofil und die Zertifikate sowie die jeweilige Anzeige aus Nutzersicht dargestellt.

Mit Version 2.2 wurde das Schnelltestprofil eingeführt (siehe D-2-3), mit Version 2.3 die Funktion zur Anzeige der Impfbzertifikate in der CWA (siehe D-2-4), ab Version 2.4 ist es dem CWA-Nutzer möglich, auch Testzertifikate für seine Tests anzufordern (siehe D-2-5) und mit Version 2.5 Genesenzertifikate (siehe D-2-6). Zudem wird nun eine Funktion zur Verwaltung der Zertifikate von Familienmitgliedern in der CWA implementiert (siehe D-2-7).

A. Allgemein

Durch die Corona-Pandemie kam es zu dem weltweiten Ausbruch der neuen Atemwegserkrankung COVID-19 („Corona“). Verursacht wird die Erkrankung durch eine Infektion mit dem bis bisher unbekanntem Coronavirus SARS-CoV-2. In zahlreichen Ländern der Welt gab es im Verlauf der Pandemie massive Einschnitte in das öffentliche Leben und in das Privatleben vieler Bürger. Zur Unterstützung der frühestmöglichen Unterbrechung der Infektionsketten wurde die Corona-Warn-App entwickelt. Hierzu sollen die Benutzer durch die CWA App über den Kontakt zu einer infizierten Person möglichst früh gewarnt und bei dem Erhalt ihres Testergebnisses unterstützt werden.

Das Erfassen der möglichen Begegnungen mit infizierten Personen erfolgt durch die sog. Annäherungsverfolgung (Tracing). Ziel der Annäherungsverfolgung ist es, Benutzer darüber zu informieren, dass sie in körperlicher Nähe zu einer infizierten Person standen, ohne die Identität der infizierten Person oder den Ort, an dem dieser Kontakt stattgefunden hat, preiszugeben. Dabei geht es vor allem darum, Kontakte zu erfassen, die nicht aus dem persönlichen Umfeld stammen und von denen der Benutzer deshalb nicht erfahren kann, dass sie infiziert waren. Solche Kontakte können in öffentlichen Verkehrsmitteln, Supermärkten usw. stattfinden. Voraussetzung für die Annäherungsverfolgung ist, dass der Benutzer sein mobiles Gerät bei sich trägt, die CWA App installiert ist und er die Bluetooth Schnittstelle aktiviert hat. Denn über die Bluetooth Schnittstelle sendet der Benutzer Zufalls-IDs und empfängt die Zufalls-IDs anderer Benutzer. Durch ein von Google und Apple bereitgestelltes Framework, auf das die CWA App zugreifen kann, wird berechnet, ob bei einem der Kontakte ein besonderes Risiko für eine Ansteckung bestand. Die Algorithmen für die Berechnungen werden von dem Robert Koch-Institut (RKI) zur Verfügung gestellt und entsprechen den neusten wissenschaftlichen Erkenntnissen. Das Ergebnis der Risikoeinschätzung wird dem Benutzer mit entsprechenden Handlungsempfehlungen auf dem mobilen Gerät angezeigt. Die weitere allgemeine Beschreibung, insbesondere der Phasen I. (Idee) bis IV. (Deinstallation) sind in den Designentscheidungen a. beschrieben.

Nachfolgend werden unter B. die Einbindung der Schnelltesteinrichtungen und unter C. speziell die Phasen der Anwendungen zur Antigen-Schnelltestregistrierung, Warnung und Anzeige beschrieben. Unter D. werden die digitalen COVID-Zertifikate nach der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates vom 14. Juni 2021 über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion (digitales COVID-Zertifikat der EU) mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie (DCC-VO) beschrieben.

B. Point-of-Care (PoC): Portallösung und Antigen-Schnelltest-Schnittstelle für Drittanbieter

Die Schnelltesteinrichtungen, sog. „Point-of-Care“ (PoC), sind eigene Verantwortliche für die Verarbeitung in ihren Systemen (PoC-Frontend/ PoC-Backend). Dies liegt nicht im Verantwortungsbereich der Corona Warn App. Die technische Ausgestaltung der Lösung kann daher anbieterspezifisch ausfallen.

Es werden den PoC zwei Möglichkeiten zur Anbindung an die CWA zur Verfügung gestellt. Zum einen die sog. Portallösung für alle PoC, die keine eigene Softwarelösung haben. Die Portallösung beinhaltet die Zurverfügungstellung von Front- und Backend durch die Telekom (verantwortlich bleibt der PoC). Zum anderen: die Antigen-Schnelltest-Schnittstelle zur Systemintegration von Drittanbietern, die bereits eigene Systeme zur Verwaltung von Patienten und Testergebnissen haben.

Die Anbindung der Point-of-Care (Poc) an die CWA erfolgt wiederum in beiden Fällen auf der Ebene der Anbindung eines jeweiligen PoC-Backends des Anbieters mittels Bereitstellung einer Schnittstelle (POC REST-API) an die CWA.

C. Testregistrierung: Übertragung von Antigen-Schnelltestergebnissen in die CWA

Für den CWA-Nutzer gibt es zwei Möglichkeiten, sein Schnelltestergebnis in die CWA zu übertragen. Die erste Option ist die, dass der CWA-Nutzer eine E-Mail mit einem Link erhält. Sofern der Nutzer auf den Link klickt und die CWA App auf dem Smartphone nicht installiert ist, wird der Nutzer auf den jeweiligen App Store des Betriebssystems Anbieters weitergeleitet. Wenn die CWA bereits installiert ist, werden die Daten zum Schnelltest direkt an die CWA App übergeben. Alternativ kann er einen QR-Code bekommen, den er über die CWA App einscannen kann.

Der Betroffene kann sich entscheiden, ob er eine pseudonymisierte Übermittlung wünscht oder eine personalisierte.

C.1. Pseudonymisierte Übermittlung des Antigen-Schnelltestergebnisses

Im Rahmen der Probenentnahme erteilt der Betroffene beim Point of Care (PoC) die Einwilligung zur pseudonymisierten Übermittlung des Testergebnisses.

Der PoC stellt dem Betroffenen daraufhin einen E-Mail Link oder QR-Code mit der CWA Test ID und dem Testzeitpunkt zur Verfügung. Nachdem der Benutzer den QR-Code mit der CWA App gescannt hat, verbindet sich das mobile Gerät mit dem sogenannten Verification Server der CWA. Dieser Server ist für den Verifikationsprozess verantwortlich. Der Verification Server speichert die in dem QR-Code enthaltene Hash (CWA Test ID) und gibt an die CWA App eine neue ID

zurück, den Registration Token. Die weitere Kommunikation zwischen dem Verification Server und der CWA App findet nur noch über den Austausch des Registration Token statt. Damit soll erreicht werden, dass der QR-Code nur für ein mobiles Gerät verwendet werden kann. Damit kann auch das Testergebnis nur von diesem mobilen Gerät abgefragt werden. Das PoC-Backend überträgt mittels des Hash (CWA Test ID) das Testergebnis zur POC REST API. Die PoC REST API prüft das Testergebnis auf Einhaltung des für Antigentestergebnisse reservierten Wertebereichs. Im Erfolgsfall überträgt die POC REST API das Testergebnis an den Test Result Server der CWA. Von diesem kann das Testergebnis durch die CWA App abgerufen werden, indem die CWA App das Registration Token für einen Request dem Verification Server bereitstellt, der mit dem Hash (CWA Test ID) aus der Testregistrierung das Testergebnis abrufen und der CWA App bereitstellt.

C.2. Personalisierte Übermittlung des Antigen-Schnelltestergebnisses

Für die personalisierte Übermittlung des Testergebnisses erteilt der Betroffene eine Einwilligung, die zusätzlich zu CWA Test ID und Testzeitpunkt die Übermittlung von Name, Vorname, Geburtsdatum, PoC interner TestID und Salt-Wert im QR-Code umfasst. Die CWA App errechnet aus den personenbezogenen Daten und dem Salt-Wert erneut die CWA Test ID, um sicherzustellen, dass die angezeigten Daten dem abzurufenden Testergebnis zugeordnet werden können.

Mittels der sich ergebenden CWA Test ID registriert die CWA App wie im Falle der pseudonymisierten Übermittlung des Testergebnisses und ruft das Testergebnis ab. Ebenso erfolgt die Übermittlung des Testergebnisses durch das PoC-Backend wie im Falle der pseudonymisierten Übermittlung des Testergebnisses in die CWA.

Der Benutzer muss den digitalen Testinformationsprozess nicht nutzen. Er kann nach wie vor auf analogem Weg von seinem Arzt oder dem Gesundheitsamt benachrichtigt werden.

B.3. Anzeige von Schnelltestergebnissen in der CWA – App

Sofern der CWA-Nutzer dies wünscht, kann er über die CWA App seinen persönlichen Infektionsstatus nachweisen (z.B. negativer Schnelltest). Es ist allerdings zu beachten, dass der CWA-Nutzer die CWA App nicht für diese Zwecke als Nachweis nutzen muss. Der Infektionsstatus des CAW-Nutzers kann im Rahmen von rechtlichen Bestimmungen (des jeweiligen Aufenthaltsortes) auch auf andere Weise nachgewiesen werden.

B.4 Warnung auslösen

Auch die Schnelltestergebnisse kann ein CWA-Nutzer zum Warnen anderer verwenden.

Im Fall eines positiven Corona-Tests kann der Benutzer freiwillig die in dem Framework (ENF) von Google und Apple gespeicherten, täglich an ihn vergebenen Zufalls-IDs der letzten 2 Wochen veröffentlichen. Weil der Benutzer selbst infiziert ist, heißen diese Tagesschlüssel von nun an Positivschlüssel.

Wenn der Benutzer sein positives Schnelltestergebnis mit der CWA App abgerufen hat, wird er gefragt, ob er seine Positivschlüssel auf den Server laden möchte, um anderen mitzuteilen, dass sie sich angesteckt haben könnten. Wenn der Benutzer zustimmt, generiert der Verification Server eine TAN und sendet diese an

die CWA App. Die TAN wird als Autorisierung und Beweis dafür, dass ein positives Testergebnis vorliegt, mit den Positivschlüsseln der letzten 2 Wochen auf einen anderen Server des Systems, den CWA Server, geladen. Der CWA Server nimmt die TAN und fragt bei dem Verification Server an, ob die TAN valide ist. Dieser antwortet entsprechend. Nur, wenn eine positive Bestätigung durch den Verification Server vorliegt, speichert der CWA Server die Positivschlüssel in der Datenbank. Falls der Upload fehlschlägt, erhält der Benutzer eine entsprechende Rückmeldung, dass die Daten erneut eingereicht werden müssen.

Positivschlüssel auf Basis von Schnelltestergebnissen werden nicht an das EFGS oder das Schweizer-Gateway (CHGS) übermittelt.

D. Digitale COVID-Zertifikate: Verwalten der Zertifikate in der CWA

Die zunächst mit § 22 Abs. 5-7 IfSG und mit der DCC-VO am 01.07.2021 EU-weit eingeführten digitalen COVID-Zertifikate der EU können in der CWA App gespeichert und angezeigt werden. Mit der IfSG-Novellierung wurden drei Kategorien von digitalen Zertifikaten eingeführt, mit denen Personen nachweisen können, dass von Ihnen keine bzw. eine nur geringe Ansteckungsgefahr ausgeht, nämlich Impfzertifikate (§ 22 Abs. 5 IfSG), Genesenenzertifikate (§ 22 Abs. 6 IfSG) und Testzertifikate (§ 22 Abs. 7 IfSG). Durch die nationale Regelung der digitalen Zertifikate im IfSG wurde sichergestellt, dass die in Deutschland im Laufe des Monat Juni ausgestellten Zertifikate auch nach dem Inkrafttreten der DCC-VO am 01.07.2021 EU-weit nutzbar sind. Die digitalen COVID-Zertifikate werden auf Wunsch des Geimpften, Getesteten oder Genesenen ausgegeben und enthalten jeweils einen QR-Code, der das eigentliche digitale COVID-Zertifikat darstellt. Dieser QR-Code enthält in maschinenlesbarer Form Angaben zur Impfung/Testung/Genesung sowie den Namen und das Geburtsdatum des Zertifikatsinhabers. Seit dem Release 2.4 werden auch die mit § 22 Abs. 7 IfSG eingeführten COVID-19-Testzertifikate in der CWA App gespeichert und angezeigt werden können. Seit dem Release 2.5 werden auch die mit § 22 Abs. 6 IfSG eingeführten COVID-19-Genesenenzertifikate unterstützt.

Jedes COVID-Zertifikat enthält einen QR-Code, der in maschinenlesbarer Form die Angaben zum Impf- bzw. Test- bzw. Genesenenstatus sowie den Namen und das Geburtsdatum des Zertifikatsinhabers enthält. Der CWA-Nutzer kann das COVID-Zertifikat in Papierform sowie in digitaler Form in einer App verwenden. Nachweise können außer mit den COVID-Zertifikaten auch in anderer Form erbracht werden (z.B. mit dem gelben Impfausweis).

Um ein COVID-Zertifikat elektronisch mit der CWA App zu nutzen, muss der CWA-Nutzer den QR-Code des COVID-Zertifikats mit der CWA App scannen. Dabei werden die Daten des COVID-Zertifikats ausgelesen und lokal im App-Speicher gespeichert. Nach dem Scannen eines COVID-Zertifikats wird es in der einer Liste der bisher gescannten COVID-Zertifikate angezeigt.

Wenn der CWA-Nutzer seinen Impf- bzw. Test- bzw. Genesenenstatus mit einem in der CWA App gespeicherten COVID-Zertifikat gegenüber Dritten (z. B. Grenzbehörden, Dienstleistern) nachweisen möchte, kann er den QR-Code des betreffenden COVID-Zertifikats auf dem Bildschirm seines Smartphones großformatig anzeigen lassen und diesen dann der Prüfperson vorlegen. Die Prüfperson kann den QR-Code sodann mit einer speziellen Prüf-Anwendung (z. B. CovPassCheck-App des RKI) scannen und auslesen. Dem Prüfer wird in der Prüf-Anwendung angezeigt, ob das vorgelegte COVID-Zertifikats (in Gestalt des QR-Codes) gültig und ggf. der Impfschutz vollständig ist bzw. ein gültiges Genesenenzertifikat vorliegt, wobei zwischen diesen Zertifikaten bei der Anzeige des Prüfergebnisses nicht unterschieden wird. Testzertifikate mit negativem Testergebnis werden als solche ausgewiesen und das Alter des Tests angegeben. Zusätzlich werden stets der Name und das Geburtsdatum des Zertifikatsinhabers in der Prüf-Anwendung angezeigt, so dass eine prüfende Person in Verbindung

mit einem Identitätsnachweis des CWA-Nutzers (z. B. Personalausweis oder Reisepass) prüfen kann, ob der CWA-Nutzer tatsächlich die Person ist, auf die sich das von ihm vorgelegte COVID-Zertifikat bezieht.

Es können auch COVID-Zertifikate von Familienmitgliedern in der CWA App gespeichert und verwaltet werden.

G. Designentscheidungen

Nachfolgend werden die Designentscheidungen dargestellt, mit denen den Bedrohungen für die Rechte und Freiheiten der Benutzer der CWA App begegnet wurde. Dabei werden hier nur die spezifischen Designentscheidungen aufgeführt, die infolge der PoC-Anbindung und der Zweckerweiterung (Ermöglichung der Nachweiserbringung über den eigenen Infektions-/ Impfstatus, der Anforderung von Testzertifikaten, Anzeige von Genesenenzertifikaten sowie der Funktion für Familienzertifikate) getroffen wurden. Im Übrigen gelten zusätzlich die Designentscheidungen a.).

Gelbe Markierungen sind noch nicht umgesetzt

I. Bedrohungen für den Datenschutz

1. Zweckgebundenheit & Epidemiologischer Sinn

Nachfolgend wird dargestellt, wie die Zweckgebundenheit durch grundsätzliche Designentscheidungen umgesetzt wurde.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
Zweckgebundenheit & Epidemiologischer Sinn Die Verarbeitung von personenbezogenen Daten ist immer an einen Zweck gebunden.	D-1-1		Das Robert Koch-Institut (RKI) hat für den Einsatz der App klarstellend und ergänzend zu den ursprünglichen Zwecken (siehe Designentscheidungen a.), D-1-1) mit Release 2.1 die folgenden Zwecke verbindlich festgelegt:	DSK Rahmenkonzept v2.1, Kapitel 8



Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
<p>Dieser muss vor der Datenverarbeitung ganz konkret festgelegt werden und kann nicht beliebig ausgetauscht werden. Außerdem muss der Zweck auch erreichbar sein. Die Datenverarbeitung darf also nicht mit einem utopischen Ziel gerechtfertigt werden.</p>			<ul style="list-style-type: none"> ✓ Der Benutzer soll automatisch darüber informiert werden, ob er Kontakt zu einer infizierten Person hatte und ob wegen der Dauer des Kontakts und des Abstands zu der Person ein Infektionsrisiko besteht. ✓ Dem Benutzer sollen durch die CWA App (auf Basis der aktuellen Empfehlungen des RKI) Informationen zu seinem Infektionsrisiko und Empfehlungen zu Gesundheits- und Infektionsschutzmaßnahmen bereitgestellt werden, um Infektionsketten möglichst frühzeitig zu unterbrechen. ✓ Soweit der CWA-Nutzer es wünscht, soll er durch die CWA App möglichst schnell und direkt auch über sein Schnelltestergebnis informiert werden, so dass er ohne Zeitverlust Maßnahmen zur eigenen Gesundheitsfürsorge und zur Reduzierung des Ansteckungsrisikos für andere Personen ergreifen kann. ✓ Soweit der CWA-Nutzer es wünscht, kann er auch sein positives Schnelltestergebnis für die Gemeinschaft verfügbar machen, so dass andere darüber informiert werden können, dass sie sich in 	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
			<p>unmittelbarer Nähe zu einer infizierten Person aufgehalten haben.</p> <ul style="list-style-type: none"> ✓ Soweit der CWA-Nutzer es wünscht, soll er über die CWA App den Nachweis über den eigenen Infektions-/ Impfstatus digital erbringen können. ✓ CWA-Nutzer sollen bei der niedrigschwelligen Inanspruchnahme von präventiven Coronatests unterstützt werden. ⚠ Es ist allerdings zu beachten, dass der CWA-Nutzer die CWA App nicht als Nachweis nutzen muss. Der Infektions-/Impfstatus des CWA-Nutzers kann im Rahmen von rechtlichen Bestimmungen (des jeweiligen Aufenthaltsortes) auch auf andere Weise nachgewiesen werden. 	




2. Zweckerfüllende Funktionalität der App

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Zweckentsprechende Funktionalität der CWA App</p> <p>Um ihren Zweck erfüllen zu können, muss die CWA App auch die entsprechende Funktionalität zur Registrierung, Verwaltung, Anzeige und Warnung im Zusammenhang mit Antigen-Schnelltests aufweisen.</p>	D-2-1		<p>Funktion: Information an Benutzer</p> <p>✓ Die CWA App informiert den Benutzer darüber, dass er einem Infektionsrisiko ausgesetzt war. Diese Information beruht auf den Berechnungen, die das mobile Gerät anhand der zuvor festgelegten Parameter lokal durchgeführt hat. Das Framework, das diese Berechnungen vornimmt, heißt Exposure Notification Framework (ENF) und wird von Google und Apple im Betriebssystem bereitgestellt. Die CWA App selbst nimmt die Berechnungen nicht vor und erhält nur das Ergebnis. Der primäre Parameter für die Berechnung, ob es zu einer Ansteckung gekommen sein kann, ist die räumliche Nähe zu einem infizierten Benutzer innerhalb eines Zeitfensters von 2 Wochen vor dessen positivem Testergebnis (der Wert für das Zeitfenster wird von den Gesundheitsbehörden festgelegt).</p>	<p>Scoping document.md – Github E04.01</p> <p>DSK CWA App v2.1, 4.4.2, 6.4, 7.1.6, 6.7, 6,9.2,</p>



Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-2-2		<p>Handlungsempfehlungen für den Benutzer</p> <ul style="list-style-type: none"> ✓ Die App gibt dem Benutzer Empfehlungen, wenn berechnet wurde, dass er einem Infektionsrisiko ausgesetzt war. Neben den Empfehlungen bekommt der Benutzer Informationen darüber, wie er weiteren Rat einholen kann. Des Weiteren kann er über den FAQ Link zu weiterführenden Informationen zum Ablauf eines Corona Test gelangen oder an einer Befragung des RKI zur CWA App teilnehmen (EDUS). <p>Informationen über Antigen-Schnelltests</p> <ul style="list-style-type: none"> ✓ Im Rahmen der Probeentnahme für Antigen-Schnelltest erhält der CWA-Nutzer Informationen von den Point of Care (PoC). ✓ Soweit auf Wunsch des CWA-Nutzers ein Schnelltest in die CWA App hinzugefügt wurde, wird über den Home-Screen der CWA App eine neue Kachel angezeigt, die dem CWA-Nutzer Informationen zum Schnelltest bereitstellt. 	<p>Scoping document.md – Github E04.02,</p> <p>DSK_CWA App v2.1, Kap. 6.2</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Anzeige im Kontakttagebuch</p>			<p>Die CWA App kann maximal einen Schnelltest und einen PCR-Test gleichzeitig verwalten. Wenn ein weiterer Schnelltest registriert werden soll, wird der erste Schnelltest aus der CWA App gelöscht.</p> <p> Für Schnelltests gibt es kein TeleTAN-Verfahren. Dieses steht nur für PCR-Tests zur Verfügung.</p> <p>Anzeige von PCR-Tests und Schnelltests im KTB</p> <p>Die Ergebnisse der durchgeführten Corona Tests (PCR/Schnelltest) werden im Kontakt-Tagebuch angezeigt. Das Kontakt-Tagebuch bietet dem CWA-Nutzer einen Überblick über die verschiedenen Testergebnisse.</p>	<p>DSK CWA App v2.1, Kap. 6.6</p>
<p>Schnelltest-Profil</p> <p>Die CWA App ermöglicht es dem CWA-Nutzer ab Release 2.2 ein Schnelltest-Profil in der CWA App anzulegen und zu verwalten. Damit kann sich der CWA-</p>	<p>D-2-3</p>		<p> Die Nutzung des Schnelltest-Profiles ist für den CWA-Nutzer freiwillig. Die von der Teststelle benötigten Informationen können auch durch die Mitarbeiter der Teststelle erfasst werden.</p>	<p>DSK CWA-App v2.2, 6.1, 6.4.2 f.</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Nutzer per QR-Code schnell und einfach bei einer Teststelle registrieren, sofern diese das Einlesen der entsprechenden QR-Codes der CWA App unterstützen.			Im Schnelltestprofil können (nur) folgende Daten eingegeben werden: Vorname, Nachname, Geburtsdatum, Wohnort, Straße, Hausnummer, Postleitzahl, Telefonnummer, E-Mail-Adresse.	
<p>Anzeige von Impfzertifikaten (Wallet Funktion)</p> <p>Mit Release 2.3 der CWA App wird es dem CWA-Nutzer ermöglicht, Impfnachweise in der CWA App zu registrieren und zu verwalten. Fügt der CWA-Nutzer seine Impfnachweise in die CWA App hinzu, können diese dem CWA-Nutzer angezeigt werden (QR-Code + Details auf dem entsprechenden Screen).</p>	D-2-4		<p>✓ Die Nutzung dieser Funktionalität durch den CWA-Nutzer ist freiwillig.</p> <p>Die Grundlage der Datenstruktur ist das definierte „EU Digital COVID Certificate“ (inkl. Vorname, Name, Geburtsdatum, Impfstoff, Impfdatum).</p> <p>⚠ Die CWA App fungiert als Wallet App. Daher findet aktuell keine Prüfung statt, ob es sich um einen gültigen Impfnachweis handelt oder nicht. Eine Überprüfung des Impfnachweises auf Gültigkeit erfolgt über eine dafür freigebende Anwendung zur Verifikation von Impfnachweisen.</p>	DSK CWA App v2.3, 7.4.17 + Tabelle 45 (DGC JSON-Schema)
<p>Anforderung/ Anzeige von Testzertifikaten für negative Tests (Wallet Funktion)</p>	D-2-5		<p>⚠ Die CWA – App fungiert auch hinsichtlich der Integration von Testzertifikaten als reine Wallet-App, die Zertifikate hält, aber nicht deren Gültigkeit und Echtheit prüft. Dies ist eine Folge der</p>	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Die CWA App ermöglicht es dem CWA-Nutzer mit Release 2.4 auch Testzertifikate für seine Tests anzufordern. Die CWA-App ermöglicht es ausschließlich für einen negativen Test ein Testzertifikat anzufordern.</p> <p>Der CWA-Nutzer kann über die CWA App ein offizielles digitales Testzertifikat anfordern und anschließend in der CWA App hinzufügen.</p> <p>Dieses digitale Testzertifikat (QR-Code) kann innerhalb der EU verwendet werden, um ein negatives Testergebnis nachzuweisen (z.B. für Auslandsreisen).</p> <p>Das Signieren von negativen Testergebnissen, mithin die Zertifikatserstellung gemäß den Vorgaben der DCC-VO, bedingt auch Erweiterungen im Bereich des Verifikationsservers, um diese Funktionalitäten zu gewährleisten.</p>			<p>Designentscheidung, dass in der CWA keine Klardaten verarbeitet werden (Siehe unten, 5-1-8).</p> <p>Eine Prüfung der Zertifikate erfolgt durch eine dafür freigegebene Anwendung zur Verifikation von Test- und Impfnachweisen (Verifier App) .</p> <p> Um in der Verifier App den Typ des Zertifikates unterscheiden zu können, soll durch die CovPass-App das von der DCC-VO der EU spezifizierte Feld „extended key usage“ implementiert werden und die Funktion in der CWA erst dann zur Verfügung stehen.</p> <p> Die Nutzung der Funktionalität ist für den CWA-Nutzer freiwillig. Er kann selbst entscheiden, ob er ein Testzertifikat anfordern möchte oder nicht.</p> <p> Nicht jede Teststelle unterstützt die Ausstellung von Testzertifikaten.</p> <p>a. Testzertifikat für Antigen-Schnelltests</p> <p>Wenn die CWA App ein validen QR-Code für die Abfrage eines Testergebnisses erkennt und die notwendigen Datenfelder für den Empfang eines Testzertifikates vorliegen, dann wird dem CWA-Nutzer der Screen „COVID-19-Testzertifikat“</p>	<p>DSK CWA-App v2.4, 7.4.19</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>angezeigt. Dieser Screen informiert den CWA-Nutzer über die wesentlichen Details zur Nutzung der Testzertifikate in der CWA App.</p> <p>Der CWA-Nutzer kann sich an dieser Stelle dann entscheiden, ob er ein Testzertifikat für seinen Schnelltest erhalten möchte oder nicht. Der CWA-Nutzer wird daraufhin über verschiedene Screens über die weiteren Schritte informiert.</p> <p>Sofern die Teststelle die Erstellung von Testzertifikaten nicht unterstützt, gelangt der CWA-Nutzer direkt zum Screen „Ihr Testergebnis“.</p> <p>Nachdem der CWA-Nutzer sein negatives Testergebnis erhalten hat und der CWA-Nutzer sein Testzertifikat für den Test angefordert hat, muss sich die CWA App beim DCC Server entsprechend registrieren.</p> <p>Zur Registrierung des Testzertifikats erzeugt die CWA App für den Test einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel wird zusammen mit dem Registration Token von der CWA App an den DCC Server übermittelt.</p>	<p>DSK CWA-App v2.4, 6.4.1 Abbildungen 26-28</p> <p>DSK CWA-App v2.4, 6.5.3</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>Anschließend fordert die CWA App regelmäßig das Testzertifikat vom DCC Server an, bis dieses zur Verfügung steht. Sofern das Testzertifikat zur Verfügung steht, wird dieses an die CWA App weitergeleitet. Das Testzertifikat wird in der CWA App persistiert.</p> <p>b. Testzertifikate für PCR-Tests</p> <p> Damit ein CWA-Nutzer ein Testzertifikat erhalten kann, muss er dies bei der Test-Registrierung angeben. Aus technischen Gründen kann er dies später nicht mehr nachholen.</p> <p>Entscheidet sich der CWA-Nutzer ein Testzertifikat anzufordern, muss der CWA-Nutzer sein Geburtsdatum in die CWA App eingeben und anschließend den Button „Testzertifikat anfordern“ antippen. Die CWA App versucht nun im Hintergrund das Testzertifikat für den registrierten PCR-Test einzuholen.</p> <p> Zusätzliches Datum zur Dublettenvermeidung</p> <p>Zur Vermeidung von Dubletten wird zusätzlich zur GUID, welche aus dem QR-Code entnommen wird, das Geburtsdatum der zu testenden Person in die</p>	<p>DSK_Verifikation/ Testresult v 2.4, 3.1.2.3</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>Generierung des Hash-Wertes mit aufgenommen. Dieses zusätzliche Datum ist dem Labor und dem CWA-Nutzer bekannt und dient der zusätzlichen Absicherung der Abfrage von PCR Testergebnissen.</p>	
<p>Anzeige von Genesenzertifikaten (Wallet Funktion)</p> <p>Mit Release 2.5 der CWA App wird dem dem CWA-Nutzer ermöglicht ein Genesenzertifikat in der CWA App zu registrieren und zu verwalten.</p> <p>Zur Registrierung des Zertifikates muss der CWA-Nutzer über die Tab-Navigation in den Abschnitt Zertifikate wechseln. Von dort kann dieser über den Button „Zertifikat hinzufügen“ ein Genesenzertifikat hinzufügen. Nachdem der CWA-Nutzer ein Genesenzertifikat in der CWA App hinzugefügt hat, wird dem CWA-Nutzer dieses in der Liste der hinterlegten</p>	D-2-6		<p><u>Anzeige von Genesenzertifikaten</u></p> <ul style="list-style-type: none"> ✓ Die Nutzung der Funktion ist für den CWA-Nutzer freiwillig. ⚠ Die CWA – App fungiert auch hinsichtlich der Anzeige von Genesenzertifikaten als reine Wallet-App, die Zertifikate hält, aber nicht deren Gültigkeit und Echtheit prüft. <p>Die Registrierung eines Genesenzertifikat wird durch das Scannen eines QR-Codes für ein Genesenzertifikats (digitales DCC) ausgelöst. Nach Prüfung auf Dubletten wird der Datensatz aus dem QR-Code in der CWA App gespeichert.</p>	DSK CWA App v2.5, 6.17.3; 7.4.18.3.6.3

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Zertifikate angezeigt. Durch „Antippen“ des Genesenenzertifikates kann der CWA-Nutzer sich weitere Informationen zu dem Genesenenzertifikat ansehen.</p>			<p>Sofern beim Speichern des Datensatzes zum Genesenenzertifikat ein Fehler passiert, wird dies dem CWA-Nutzer über eine entsprechende Fehlermeldung angezeigt.</p> <p>Verwaltung der verschiedenen Zertifikate in der CWA App</p> <p>Der CWA-Nutzer kann in der CWA App ein bevorzugt anzuzeigendes Zertifikat markieren. Dieses wird dem CWA-Nutzer als erstes Zertifikat in der Liste der eingescannten Zertifikate angezeigt. Die anderen vorhandenen Zertifikate werden nach einer Wertigkeitsreihenfolge in der Liste der vorhandenen Zertifikate angezeigt. Die Wertigkeitsreihenfolge gibt an, an welcher Stelle ein bestimmtes Zertifikat aus der Liste der verfügbaren Zertifikate angezeigt wird. Die Wertigkeitsreihenfolge erfolgt anhand eines vom RKI definierten Regelwerks.</p>	<p>DSK_CWA_App v2.5, 7.4.18.3.7</p>
<p>Funktion für Familienzertifikate</p> <p>Mit Release 2.5 der CWA App wird es dem CWA-Nutzer ermöglicht, COVID-Zertifikate</p>	<p>D-2-7</p>		<p>✓ Die Nutzung der Funktion ist für den CWA-Nutzer freiwillig.</p>	<p>DSK CWA App v2.5, 7.4.22</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>anderer Personen, bezweckt seiner Familienmitglieder, in seiner CWA App zu registrieren und zu verwalten. Diese Funktion erlaubt es dem CWA-Nutzer die Zertifikate seiner Familienmitglieder z.B. bei einer Auslandsreise vorzuzeigen.</p>			<p>Der CWA-Nutzer kann unter dem Tab-Menü „Zertifikate“ weitere Zertifikate in die CWA App hinzufügen, indem dieser auf den Button „Zertifikat hinzufügen“ tippt und die entsprechenden QR-Codes mit der CWA einscann.</p> <p>Die Daten werden im Speicher der CWA App zusammen mit den Daten zu den Zertifikaten vom CWA-Nutzer gespeichert. Beim Öffnen des Tabs „Zertifikate“ werden die Daten zu den Zertifikaten aus den in der CWA App gespeicherten Zertifikaten geladen und dem CWA-Nutzer angezeigt.</p>	

2.1 Fehlfunktion

Folgende Designentscheidungen/ Bewertungen dienen verschiedenen Datenschutzschutzziele (Transparenz, Vertraulichkeit...) durch die Vermeidung von Fehlfunktionen der CWA.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Sicherheitslücken Open Source Komponenten</p> <p>Sicherheitslücken in Open Source Software Komponenten können, soweit sie die Funktionalität der CWA App einschränken oder das Vertrauen der Benutzer in die Sicherheit der App beschädigen dazu beitragen, dass der Zweck der App nicht erreicht werden kann. Deshalb ist es wichtig, dass ein geordneter Prozess für den Umgang mit Sicherheitslücken besteht.</p>	D-2.1-2		<p>Umgang mit Sicherheitslücken</p> <p>✓ Um das Risiko durch Sicherheitslücken in verwendeten Open Source Software Komponenten möglichst gering zu halten, werden die eingesetzten Komponenten stets auf dem neuesten Stand gehalten. Dabei wird sowohl auf interne als auch externe Werkzeuge (wie z.B. GitHub Security Alerts for Vulnerable Dependencies und WhiteSource) zurückgegriffen. Zusätzlich werden in einer SAP-internen Pipeline im Rahmen der Programmentwicklung Source Code Scans (z.B. mit Fortify) durchgeführt, um etwaige Sicherheitslücken frühzeitig zu erkennen.</p>	DSK Rahmenkonzept, 14.18
<p>IT-Sicherheit für die Einbindung der PoC und Integration von Testzertifikaten (DCC Server)</p>	D-2.1-3		<p>✓ Die Einbindung der PoC befindet sich momentan in der Entwicklung. Es wird ein PSA-Verfahren umgesetzt, in dem auch die Überlegungen des BSI-Grundschutzes umgesetzt werden. Das PSA-Verfahren ist zum Stand 09.06.2021 noch nicht abgeschlossen. Für die Version 2.4 und die vorgesehene Datenverarbeitung mittels des DCC Servers wird ebenfalls ein PSA-Verfahren durchgeführt. Dieses ist zum Stand 10.06.2021 noch nicht abgeschlossen.</p> <p>✓ Das BSI hat vor Freigabe des Release 2.1 einen Pentest durchgeführt und einen Bericht übergeben, der</p>	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			Schwachstellen und Mitigationsmaßnahmen berücksichtigt.	

2.2 Fehlgebrauch

Nachfolgend werden Designentscheidungen und Bewertungen aufgeführt, die Risiken für betroffene Personen infolge Fehlgebrauch der CWA App und deren Funktionen (inkl. Schnelltestergebnis-Anzeige) minimieren sollen.

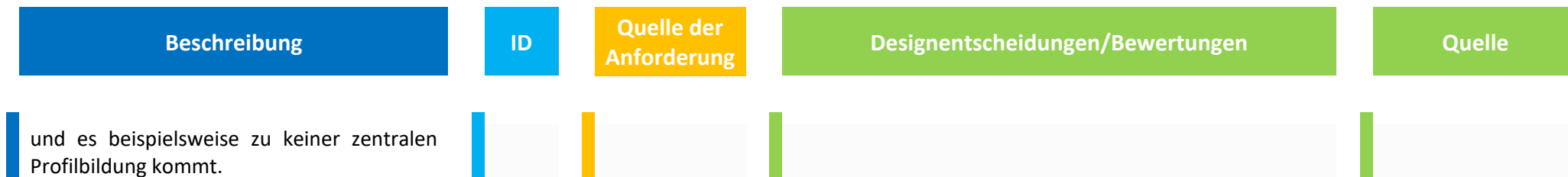
Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
Unsachgemäße Verwendung des QR-Codes	D-2.2-2		<p>Aufklärung der Benutzer über unsachgemäße Verwendung des QR-Codes</p> <p>⚠ Die CWA-Nutzer und PoC-Mitarbeiter können durch geeignete Informationen und Aufklärungskampagnen zu einer ordnungsgemäßen Nutzung aufgefordert und angeleitet werden.</p>	
Fehlerhafter Scan	D-2.2-3		Fehlermeldung an den CWA – Nutzer	DSK CWA App v2.1, 7.4.15.1

2.3 Vertrauensverlust der Bevölkerung in Vertrauenswürdigkeit der App

Da die CWA auf der Freiwilligkeit und Kooperationsbereitschaft möglichst eines Großteils der Bevölkerung beruht, müssen die Designentscheidungen dem Ziel dienen, einen Vertrauensverlust der Bevölkerung zu vermeiden. Dies gilt auch für die Schnelltest-Anbindung und Nachweisfunktion.

Nachfolgend sind die entsprechenden Designentscheidungen und Bewertungen aufgeführt.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Vermeiden von Sicherheitslücken und Datenschutzvorfällen</p> <p>Um das Vertrauen der Bevölkerung in die Sicherheit der App und die Gewährleistung des Datenschutzes nicht zu verlieren bzw. zu gewinnen, sind eine Reihe von öffentlichkeitswirksamen Maßnahmen notwendig. Insbesondere ist es hilfreich, wenn die CWA App einschließlich ihrer Infrastruktur von unabhängigen Sicherheitsforschern überprüft werden kann. Diese können gegenüber der Presse und in eigenen Veröffentlichungen zudem belegen, dass tatsächlich nur die notwendigsten Datenverarbeitungen vorgenommen werden</p>	<p>D-2.3-1</p>		<p>Open-Source</p> <p>✓ Alle Komponenten der CWA, ausgenommen dem CDN der OTC sowie der Labor-Einbindung, sind Open-Source. Die Community kann so an der Sicherheit der App mitarbeiten und ihre Funktionsweise prüfen.</p>	<p>Solution Architecture.md – GitHub</p> <p>Corona-Warn-App · GitHub</p>



3. Rechtmäßigkeit der Verarbeitung

Die Datenverarbeitungen durch die Nutzung und den Betrieb der CWA App müssen auf eine Rechtsgrundlage gestützt werden können, andernfalls ist die Datenverarbeitung personenbezogener Daten rechtswidrig.

Da kein Gesetz die Nutzung der CWA vorschreibt und die Datenverarbeitung regelt, wird die Datenverarbeitung in ihren verschiedenen Phasen ausdrücklich auf die Einwilligung der Nutzer gestützt. Die Nutzung der CWA App und die damit zusammenhängenden Datenverarbeitungen sollen nur aufgrund der Einwilligung des Einzelnen möglich sein. Eine Einwilligung ist nur dann wirksam, wenn sie hinreichend informiert und freiwillig erfolgt.

3.1 Freiwilligkeit der Nutzung der CWA-App / der Schnelltestanzeige und der digitalen Nachweisfunktion und der Einwilligungen in die Datenverarbeitung

Im Folgenden werden die Designentscheidungen dargestellt, die im Zusammenhang mit der Einwilligung stehen, um folgenden Risiken zu begegnen:

- Unwirksame Einwilligung aufgrund fehlender/fehlerhafter ausdrückliche Einwilligungserklärung (technischer Einwilligungsakt)
- Unwirksame Einwilligung aufgrund Nichterreichbarkeit der notwendigen Informationen (sprachliche Barrieren, fehlendes Technikverständnis)
- Unbefugte Nutzung der App durch Minderjährige unter 16 Jahre

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Verbot mit Erlaubnisvorbehalt</p> <p>Im Datenschutz besteht der Grundsatz des Verbots der Datenverarbeitung mit Erlaubnisvorbehalt.</p> <p>Die Übermittlung der Schnelltestergebnisse in die CWA müssen also auf eine Rechtsgrundlage gestützt werden können.</p> <p>Darüber hinaus erklärt der Benutzer über die CWA App seine Einwilligung für die verschiedenen Verarbeitungstätigkeiten wie in den Designentscheidungen a.), D-3.1-1. beschrieben.</p> <p>Die Einwilligung muss informiert erfolgen und freiwillig sein.</p>	D-3.1-1		<p>Einholung und Erteilung der Einwilligung in die Übermittlung von Schnelltestergebnissen in die CWA</p> <p>Wahl der CWA-Nutzer: Pseudonymisierte oder personalisierte Übermittlung des Testergebnisses</p> <p>Im PoC kann auf Wunsch des CWA-Nutzers das Schnelltestergebnis an die CWA übertragen werden. Dies erfolgt mittels eines QR-Codes, der entweder per E-Mail verschickt oder mittels der CWA-App eingescannt wird.</p> <p>Der CWA-Nutzer kann sich hierbei zwischen folgenden Varianten entscheiden:</p> <ol style="list-style-type: none"> 1. Pseudonymisierte Übertragung <p>In diesem Fall stellt das PoC dem CWA-Nutzer einen QR-Code mit der CWA Test ID und dem Testzeitpunkt zur Verfügung.</p> <ol style="list-style-type: none"> 2. Personalisierte Übertragung <p>In diesem Fall stellt das PoC dem CWA-Nutzer einen QR-Code zur Verfügung, der zusätzlich zu CWA Test ID und Testzeitpunkt auch den Namen, Vornamen,</p>	<p>Scoping document.md -- Github E01.01 und E01.02</p> <p>Scoping document.md -- Github E01.03 und E01.04</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>Geburtsdatum, PoC interne TestID und Salt-Wert umfasst.</p> <ul style="list-style-type: none"> ✓ Im Rahmen der Probeentnahme für den Antigen-Schnelltests erteilt der CWA-Nutzer jeweils die Einwilligung zur pseudonymisierten oder personalisierten Übermittlung des Schnelltestergebnisses an die CWA. ⚠ Verantwortlich für die Einholung der Einwilligung, deren Management und die Informiertheit der Einwilligenden ist der PoC. <p>Den PoC werden Datenschutzinformationen für Betroffene, Einwilligungstexte mittels der Portallösung und Muster Einwilligungstexte für Drittanbieter zur Verfügung gestellt.</p> <p>Die PoC werden über die Partnerschaftsverträge zur Einholung wirksamer Einwilligungen und deren Dokumentation verpflichtet. Verstöße können eine außerordentliche Vertragskündigung rechtfertigen.</p>	
	D-3.1-2		<p>Unbefugte Nutzung der CWA App durch Minderjährige unter 16 Jahre</p>	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>⚠ Sowohl in den Nutzungsbedingungen als auch in der Datenschutzerklärung wird daher klargestellt, dass die Nutzung der CWA App für Personen ab 16 Jahre vorgesehen ist. Dies betrifft somit auch die Übermittlung von Schnelltestergebnissen in die CWA und die digitale Nachweismöglichkeit des Infektionsstatus via CWA.</p> <p>Eine Gewährleistung und Dokumentation der Einwilligung von Erziehungsberechtigten für Kinder- und Jugendliche unter 16 Jahren liegt in der Verantwortung des PoC.</p> <p>⚠ Für die CWA App ist es nicht möglich, die unbefugte Nutzung durch Kinder und Jugendliche unter 16 Jahren und damit auch die (unbefugte) Datenverarbeitung (technisch oder organisatorisch) auszuschließen. Infolge dieser unbefugten Datenverarbeitung können auch Schäden für die Rechte und Freiheiten der Benutzergruppe entstehen.</p>	
	D-3.1-3		Erreichbarkeit/ Lesbarkeit der Informationen in der Sprache der Benutzer	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			✓ Datenschutzinformationen und Einwilligungstexte sollen in verschiedenen Sprachen zur Verfügung gestellt werden.	

3.2 Freiheitsbeschränkungen bei Nichtnutzung der Nachweisfunktion oder Freiheitsgewinne bei Nutzung der Nachweisfunktion /erzwungene Einwilligung

Die Freiwilligkeit der Einwilligung des Betroffenen ist zwingend, damit die Datenverarbeitung rechtmäßig ist. Es besteht jedoch die Gefahr, dass sich Benutzer durch Druck von außen (Arbeitgeber, Staat, Nachbarn o.ä.) zur personalisierten Übermittlung des Testergebnisses und damit dem Einsatz der Nachweisfunktion gezwungen sehen.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Erzwungene Einwilligung Knüpfen die Besitzer oder Betreiber im allgemeinen öffentlich zugänglicher Einrichtungen wie z.B. Restaurants, Bars, Ladengeschäfte, Kinos oder Kultureinrichtungen oder Behörden den	D-3.2-1	FifF DSFA S. 72	✓ Mit Release 2.1 wird die Möglichkeit vorgesehen, die Schnelltestergebnisse an die CWA zu übermitteln und damit auch Kontakte warnen zu können, ohne dass die Nachweisfunktion gewählt wird. Dies wird als gleichwertige Option (pseudonymisierte Übermittlung) durch die PoC zur Verfügung gestellt.	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Zugang zu ihrer Einrichtung an das Vorweisen des digitalen Nachweises des Infektions-/ Impfstatus in der CWA, wird damit die Freiwilligkeit der Nutzung der App und der Nachweisfunktion de facto außer Kraft gesetzt. (Quelle: DSK Rahmenkonzept, 10.23.17))			<ul style="list-style-type: none"> ✓ Durch Sensibilisierung, dass es sich bei der Nutzung durch Dritte zu Zwecken der Zutrittsbeschränkung ohne ausreichende Rechtsgrundlage, um einen bußgeldbewerten Verstoß handeln kann, sowie Kontrolltätigkeiten der Datenschutzaufsichtsbehörden der Länder könnte diesem Risiko begegnet werden. ✓ CWA – Nutzer werden darüber informiert, dass eine Nachweiserbringung – soweit gesetzlich vorgesehen – nicht über die CWA erfolgen muss. 	

3.3 Gefahr der Diskriminierung

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Unbeobachtbarkeit der Kommunikation (PoC – CWA)	D-3.3-1		Datenschutzfreundliche Voreinstellungen	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Auch wenn die Übermittlung einer Nachricht im System beobachtet wird (z. B. über die Metadaten der Kommunikation), darf daraus nicht geschlossen werden können, dass eine Person selbst infiziert ist oder Kontakt zu Infizierten hatte.</p> <p>Dies ist sowohl gegenüber anderen Benutzern als auch gegenüber Infrastruktur- und Netzbetreibern oder Angreifern, die Einblick in diese Systeme erlangen, sicherzustellen.</p>			<p>✓ Gegenüber Infrastruktur- und Netzbetreibern oder Angreifern, die Einblick in diese Systeme haben, sind die Daten der Benutzer insbesondere durch die Maßnahme zur Pseudonymisierung und zur Trennungskontrolle geschützt.</p>	

4. Transparenz

Designentscheidungen und Bewertungen in diesem Kapitel dienen vor allem dem Schutzziel der Transparenz. Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise erhoben und verarbeitet werden.

Gefahren der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten und Funktionsweise der CWA App soll begegnet werden.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Transparenz und Prüfbarkeit</p> <p>Um eine Prüfbarkeit der CWA App und Infrastruktur durch Auditoren, Aufsichtsbehörden und die kritische Öffentlichkeit zu ermöglichen, muss der vollständige Quelltext zur Verfügung stehen.</p>	D-4-1	<p>CCC, Nr. 4 EDSA Anhang GEN-3</p>	<p>Veröffentlichung des vollständigen Quelltextes</p> <p>✓ Die App und die Backend-Infrastruktur (inkl. EFGS) folgen dem Open-Source-Prinzip –lizenziert unter Apache 2.0.</p>	<p>Github Dokumentation, README.de.md unter „Über dieses Projekt“</p>
<p>Durchführung einer Datenschutzfolgenabschätzung</p> <p>Die mit der Datenverarbeitung verbundenen Risiken für Rechte und Freiheiten der von der Datenverarbeitung Betroffenen werden in einem strukturierten Verfahren zur Risikoabschätzung erfasst und bewertet. Es werden Gegenmaßnahmen festgelegt, Restrisiken bestimmt und die Ergebnisse öffentlich gemacht.</p>	D-4-2	<p>EDSA, Rn. 39</p>	<p>Durchführung einer Datenschutzfolgenabschätzung</p> <p>✓ Es wurde eine Datenschutz-Folgenabschätzung (DSFA) vor der Einführung der App durchgeführt und dann laufend überprüft und aktualisiert, soweit die Verarbeitungen als mit einem hohen Risiko behaftet eingestuft werden (Gesundheitsdaten, voraussichtliche flächendeckende Einführung, systematische Überwachung, Einsatz neuer technologischer Lösungen).</p> <p>Eine Datenschutzfolgenabschätzung wurde auch für die Anbindung der PoC und die Nachweisfunktionen (inklusive CWA v2.5) durchgeführt und wird bei Bedarf aktualisiert.</p>	<p>DSFA Bericht v2.1 nebst Anlagen</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-4-3	EDSA , Rn. 39, Anhang PRIV-6	<p>Veröffentlichung der Datenschutzfolgenabschätzung</p> <p>✓ Die Datenschutzfolgenabschätzung wird veröffentlicht.</p>	
<p>Datenschutzinformationen für CWA-Nutzer und Mitarbeiter der PoC</p> <p>Für die Schnelltestportal Gesamtlösung werden sowohl zur Information auf der Webseite (vor einem Login) und im Webfrontend Datenschutzhinweise bezüglich der Verarbeitung personenbezogener Daten sowohl für die Testpersonen als auch die Mitarbeiter der PoC (vor und nach dem Login) bereitgestellt.</p> <p>Bei der Anbindung von Drittanbietern liegt Verantwortung für die Information der betroffenen Personen bei diesen.</p>	D-4-4		<p>✓ Die Datenschutzinformationen für betroffene Personen werden für die erweiterten Funktionen ergänzt. Die Informationen stehen in den PoC zur Verfügung, aber auch im Rahmen der CWA-App.</p> <p>✓ Drittanbietern (Testcentren, Labore) können Textmuster für Datenschutzhinweise bei Bedarf zur Verfügung gestellt werden, dies gilt auch für die erweiterten Funktionen</p>	

5. Verdecktheit/ Unbeobachtbarkeit und Vertraulichkeit

Wesentliche Maßnahmen zur Sicherstellung der Bindung der Verarbeitungstätigkeiten für einen ausgewiesenen Zweck besteht im Allgemeinen darin, pseudonymisierte und anonymisierte Daten, bei denen der Personenbezug so weit wie möglich aufgehoben oder unter Bedingungen gestellt ist, zu verwenden und die Datenbestände, Kommunikationsbeziehungen und Teilprozesse dieser Verarbeitungstätigkeit von anderen Verarbeitungstätigkeiten zu trennen¹².

Dem Grundsatz der Vertraulichkeit folgend, dürfen personenbezogene Daten nur einem berechtigten Personenkreis für bestimmte Zwecke offenbar werden. Sie sind vor unbefugter Veränderung zu schützen.

5.1 Anonymität/Pseudonymität und verschlüsselte Speicherung der Pseudonyme

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Nr. 5 DSGVO).

Bei den Zufallszahlen, die auf dem Smartphone kreiert werden, und für die CWA erforderlich sind, handelt es sich um personenbezogene Daten im Sinne der DSGVO, da ein Personenbezug mit dem Gerätenutzer herstellbar ist. Die nachfolgende Datenverarbeitung im Rahmen der CWA erfolgt pseudonymisiert, da unmittelbare Identifizierung allein aufgrund der Zufallszahlen und ohne Bezug zu einem Smartphone erschwert wird.

Im Nachfolgenden sind die Designentscheidungen bezüglich der Pseudonymisierung im Rahmen der Übermittlung von Schnelltestergebnissen genauer dargestellt.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
	D-5.1-1		Einsatz von Verschlüsselungstechnologie ✓ Es werden hochmoderne kryptografische Techniken eingesetzt, um den Austausch zwischen der App und	GitHub - Prüfsteine für die Beurteilung von „Contact Tracing“-Apps

¹² FfF DSFA, S. 43

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			<p>den Servern sowie zwischen Anwendungen zu sichern und um generell die in den Apps und auf dem Server gespeicherten Informationen zu schützen. Etablierte Verschlüsselungsmechanismen wie E-Mail over TLS (HTTPS) stellen sicher, dass Nachrichten von außen nicht lesbar sind. Um das Risiko von Man-in-the-Middle-Angriffen weiter zu reduzieren, wird durch HTTP Public Key Pinning sichergestellt, dass vertrauliche Kommunikation nur zwischen der CWA App und dem Server stattfindet.</p> <p>Verschlüsselte Speicherung auf dem TestresultServer</p> <p>✓ Die auf dem Test Result Server liegenden Daten (Ergebnisse des Corona-Tests: Hashed GUID, Testergebnis, Datum des Imports) werden mit TLS 1.2 verschlüsselt, Kommunikation ist verschlüsselt, auf Client OS Crypto SDK implementiert.</p> <p>Damit ist sichergestellt, dass selbst Personen mit administrativen Zugriff auf die Datenbank keine Möglichkeit besitzen die Daten im Klartext vorzufinden.</p>	<p>Solution Architecture.md – GitHub DSK Verifikation und Testergebnis 4.2.4.1 – 4.2.4.4, DSK CWA Server 5.3.8</p> <p>DSK-Rahmenkonzept v1.10, Kap. 14.28.17</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
	D-5.1-2		<p>Erschwerung Re-Identifizierung durch Trennung der IT-Systeme</p> <p>✓ Die Schnelltestergebnisse werden nicht auf dem Verification Server, sondern nur auf dem Test Result Server gespeichert.</p>	<p>Solution Architecture.md – GitHub</p>
	D-5.1-3		<p>✓ Der Verification Server und der CWA Server werden von unterschiedlichen Personen und in verschiedenen Cloud Subscriptions der OTC betrieben.</p>	<p>DSK Rahmendokument, 12.5</p>
	D-5.1-4		<p>Abschirmung von Kommunikationsmustern</p>	<p>DSK CWA App, 7.3.9, DSK Rahmenkonzept, 14.14</p>
	D-5.1-5		<p>✓ Um zu verhindern, dass die gespeicherten Positivschlüssel über Netzwerkinformationen zu mobilen Geräten zugeordnet werden können, wird der Zeitstempel des Übertragungszeitpunkts auf die letzte volle vergangene Stunde abgerundet.</p>	<p>DSK CWA Server, 5.1.2</p>
	D-5.1-6		<p>✓ Die CWA App sendet (ab Release 1.2) regelmäßige vorgetäuschte Anfragen an den CWA Server. Ziel ist es zu verhindern, dass man aus dem bloßen Umstand der</p>	<p>DSK CWA Server, 5.3.10.1</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			(abgefangenen bzw. beobachteten) Kommunikation auf eine Infektion des CWA-Nutzers schließen kann	
	D-5.1-7		<p>✓ Die Server werden von getrennten Teams betrieben, um Re-Identifikationsattacken durch Admins zu erschweren.</p> <p>Für die Datenverarbeitung der PoC (Front- und Backend) sind diese verantwortlich.</p>	DSK Rahmenkonzept, 14.8
<p>Erstellung, Anforderung und Anzeige von Testzertifikaten</p> <p>Um einen namentlichen Testnachweis auch in der Form eines Testzertifikates gem. § 22 Abs. 7 Infektionsschutzgesetzes bzw. Art. 3 Abs. 2 DCC-VO zu erhalten, werden personenbezogene Daten (Name, Vorname, Geburtsdatum, Adresse der Teststelle, Zeitpunkt der Testdurchführung, Testhersteller und Name des eingesetzten Tests sowie das Testergebnis und Testzertifikatskennung) in der Teststelle sowie in der CWA-App verarbeitet.</p>	D-5.1-8		<p>✓ Auf den Serversystemen des RKI werden nur ein Hashwert der personenbezogenen Daten und die Testzertifikatskennung im Klartext verarbeitet, ansonsten sind die Daten verschlüsselt.</p> <p>Für die Generierung von COVID-Zertifikaten werden folgende Schritte durchlaufen:</p> <ol style="list-style-type: none"> 1. Initiierung durch CWA-Nutzer Der CWA-Nutzer entscheidet sich auf seinem Smartphone, dass ein COVID-Zertifikat für seinen negativen Test (PCR oder Schnelltest) erstellt werden soll. 	DSK_Verifikation und Testergebnis v2.4, 3.1.2.3

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			<ul style="list-style-type: none"> a. Eingabe des DOB Zur Sicherstellung der Dubletten Vermeidung wird hier die Eingabe des Geburtsdatums eingefordert. b. Erzeugung eines Public/Private Schlüsselpaar durch die CWA App zur Verschlüsselung aller erweiterten Testdaten, welche im weiteren Verlauf übertragen werden. <ol style="list-style-type: none"> 2. Zertifikat anfragen (Anfrage der CWA App am DCC Server) Die CWA App fragt am DCC Server bzgl. des Zertifikats, passend zum negativen Testergebnis, nach. Hierfür wird der bereits früher gebildete Registration Token und der generierte Public Key zur Verschlüsselung der Daten mitübergeben. 3. TestID abrufen (Anfrage des DCC Servers am Verifikationsserver) Der DCC Server nutzt den übertragenen Registration Token um am Verifikationsserver die passende gehashte TestID in Erfahrung zu bringen. Diese wird daraufhin am DCC Server gespeichert. 	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			<ol style="list-style-type: none"> 4. Polling nach angeforderten Zertifikaten (Anfrage des PoC an den DCC-Server) In regelmäßigen Abständen fragen die PoC-Systeme am DCC an, ob für TestIDs passend zum PoC ein Zertifikat angefordert wurde. 5. Bereitstellung von weiteren Testinformationen (Kommunikation zwischen DCC Server und PoC): Sollte eine TestID passend zum PoC ein Zertifikat anfordern, so wird im Zuge des Polling des PoC als Antwort der Public Key sowie die entsprechende TestID übermittelt. Das PoC „sammelt“ alle notwendigen Informationen für die Ausstellung eines COVID-Zertifikats und verschlüsselt diese Angaben mit dem Public Key des CWA-Nutzers. Die verschlüsselten Daten werden an das DCC rückübertragen. Damit ist sichergestellt, dass keine personenbezogenen Daten im Klartext übertragen oder gespeichert werden – diese können nur am PoC oder in der CWA App gelesen respektive entschlüsselt werden. 6. Rückübermittlung des Zertifikats an die CWA App (Übertragung von DCC Server an CWA App) Der DCC Server lässt die verschlüsselten 	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertungen	Quelle
			<p>personenbezogenen Daten über das entsprechende Issuer Backend (nicht Teil des CWA Systems) signieren und überträgt sowohl die verschlüsselten Daten als auch das Zertifikat an die CWA App.</p> <p>7. Speicherung der Daten in der CWA App Die CWA App speichert das Zertifikat sowie die mit dem public key verschlüsselten Daten. Wenn der CWA-Nutzer das COVID-Zertifikat vorzeigt, werden im Anlassfall die verschlüsselten personenbezogenen Daten entschlüsselt mithilfe des private keys und können zur Prüfung des Zertifikats herangezogen werden.</p>	

5.2 Grundlegende Privatsphäre

Nachfolgend werden Designentscheidungen zusammengefasst, die der Sicherstellung der Privatsphäre dienen.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-5.2-1		<p>✓ Die CWA App ermöglicht keine direkte Identifizierung der Benutzer.</p>	DSK Rahmenkonzept, 13.1.3
	D-5.2-3		<p>✓ Zur Pseudonymisierung der Schnelltests und damit des Benutzers wird ein QR-Code mit der CWA Test ID vergeben.</p> <p>Der Verification Server verarbeitet für Schnelltestergebnisse nur gehashte CWA Test ID.</p>	Solution Architecture.md – GitHub Software Design Verification Server
	D-5.2-6		<p>✓ Das Poc hashed die CWA Test ID und das Testergebnis.</p>	Solution Architecture.md – GitHub
	D-5.2-7		<p>✓ Personenbezogene Daten werden nur verhasht auf den Servern der CWA gespeichert.</p>	DSK Verifikation und Testergebnis 6.1.5, 6.2.5., 6.3.5.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
--------------	----	------------------------	---------------------------------	--------

6. Datensparsamkeit/ Datenminimierung

Nachfolgend werden Designentscheidungen beschrieben, die dem Datenschutzziel der Datenminimierung dienen. Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
<p>Datenanhäufung von Nutzern</p> <p>Durch eine hohe Installationsanzahl besteht die Gefahr, dass zu viele, zweckfremde Daten gespeichert werden und diese für andere Zwecke genutzt werden.</p>	D-6-1		<ul style="list-style-type: none"> ✓ Die pseudonymen Daten der Benutzer unterliegen einer strengen Zweckbindung. Die Datensätze auf dem Verification Server werden 21 Tage nach ihrer Erstellung gelöscht (Hash der GUID (PCR-Test), der CWA Test ID (Schnelltest) und Hash des Registration Token). Das Testergebnis wird auf dem Test Result Server nach 21 Tagen durch den Zustand „redeemed“ überschrieben und damit maskiert. Nach 90 Tagen wird der Datensatz endgültig gelöscht. ✓ Es dürfen nur minimale und für den Anwendungszweck notwendige Daten und Metadaten gespeichert werden. 	<p>Solution Architecture.md – GitHub</p> <p>DSK CWA Server, 5.4</p> <p>DSK CWA App, 7.4</p> <p>DSK Verifikation und Testergebnis, 6.1.6, 6.2.6</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
			<p>Mit der Einführung von Schnelltests ist es notwendig Metadaten zu den Schnelltests in der CWA zu speichern.</p>	<p>DSK CWA App, Kap. 7.4.15</p>
<p>Übertragung von nicht verarbeitungsnotwendigen Daten bei Schnittstellen</p> <p>Durch eine unsaubere Schnittstellendefinition werden zu viele Daten übertragen, welche zweckentfremdet verwendet werden können.</p>	<p>D-6-2</p>		<p>✓ Antigen-Schnelltest-Schnittstelle</p> <p>Die Anbindung der Point-of-Care – Infrastruktur an die CWA erfolgt auf der Ebene der Anbindung eines jeweiligen Backends des Anbieters („PoC-Backend“) an die CWA.</p> <p>Im Rahmen der Anbindung der PoC an die CWA-Infrastruktur werden – analog zum Laborgateway für die PCR-Tests - nur die absolut notwendigen Daten (gehashte Guid + Testergebnis) über die Rest-Schnittstelle (API) an den Test Result Server übertragen.</p> <p>✓ Für die Darstellung der Testergebnisse aus PCR-Test und aus Antigen-Schnelltest in der Datenbank des Test Result Servers sind unterschiedliche Wertebereiche vorgesehen.</p>	<p>DSK Verifikation und Testergebnis v2.1, 3.1.4.5 (Wertebereiche, Datenfeldkatalog), DSK Rahmenkonzept v2.1, 12.3.22</p>

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/ Bewertung	Quelle
			<p>✓ Die Schnittstelle wird eine Kontrolle des Wertebereichs der übertragenen Testergebnisse durchführen. Hierdurch wird eine Unterscheidbarkeit von PCR-Testergebnissen und Antigen-Schnelltestergebnissen – je nach Herkunft der Ergebnisse – sichergestellt.</p>	

7. Zweckbindung/ Nichtverkettbarkeit

Nachfolgende Designentscheidungen dienen insbesondere dem Schutzziel der Zweckbindung und dem Gewährleistungsziel der Nichtverkettung (siehe auch [CCC](#), Nr. 9). Personenbezogene Daten sind nur im Rahmen des ursprünglichen Zweckes der Verarbeitung zu verwenden und nicht mit anderen Daten zusammenzuführen. Dementsprechend darf im Laufe der Verarbeitungszwecke stets nur der ursprünglich festgelegte Zweck verfolgt werden.

Die vorgesehene Zweckerweiterung bedarf daher einer neuerlichen Datenschutzfolgenabschätzung.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Verhaltensauswertung durch die CWA Daten</p> <p>Behavioral Profiling und Compliance Scoring bei Infizierten muss vermieden werden. Betreiber können die Kontakthistorien infizierter Benutzer dazu verwenden, ein Verhaltens-Scoring zu erstellen.</p>	D-7-1		<p>✓ Die Auswertung der Kontakte und ein damit verbundenes Verhaltens-Scoring durch eine zentrale Stelle ist nicht möglich, da die Verarbeitung der Kontakte ausschließlich lokal auf dem mobilen Gerät stattfindet. Die Benutzer laden keine Kontakthistorie oder Testhistorie auf den Server.</p>	DSFA Bericht, Anhang TOMs, Ziff. 1102, 1104

8. Intervenierbarkeit

Nach dem Grundsatz der Intervenierbarkeit müssen Betroffene die Möglichkeit haben, ihre entsprechend der DSGVO gewährten Rechte ungehindert auszuüben. Datenverarbeitungen müssen so gestaltet werden, dass Daten berichtigt und gelöscht werden können. Um diesen Grundsatz im Rahmen der CWA zu genügen, müsste der Personenbezug hergestellt werden. Nachfolgend wird dargestellt, dass zur Erfüllung der Betroffenenrechte der Personenbezug nicht hergestellt wird.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Beachtung der Betroffenenrechte</p> <p>Es muss jederzeit möglich sein, Betroffenenrechte umzusetzen,</p>	D-8-1		<p>Beachtung der Betroffenenrechte</p> <p>✓ Mit der im Rahmen der CWA verarbeiteten Daten können die Benutzer nicht identifiziert werden. Daher</p>	DSK Rahmenkonzept, 11

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>insbesondere personenbezogene Daten bei Vorliegen der Voraussetzungen zu löschen, zu berichtigen und in der Verarbeitung zu beschränken.</p> <p>Auch muss es möglich sein, automatisierte Entscheidung durch den Verarbeiter prüfen zu lassen: Prozess durch den Benutzer das Ergebnis der App durch einen Menschen prüfen lassen kann.</p> <p>Durch die Anbindung der PoC und die Nachweisfunktion ändert sich nichts an den diesbezüglichen Designentscheidungen a.).</p>			<p>können Ersuchen nach Art. 15 bis 20 DSGVO nicht beantwortet werden. Die Bereitstellung von Informationen, die die Identifizierung der Benutzer ermöglichen würde, findet nicht statt. Dies würde dem Ziel zuwiderlaufen, den Gesamtprozess so datensparsam wie möglich durchzuführen. Die Art. 15 bis 20 DSGVO sind daher nicht anwendbar (Art. 11 Abs.2 DSGVO).</p> <p>✓ Der Benutzer kann die CWA App jederzeit deinstallieren und damit alle lokal gespeicherten Daten selbst löschen. Alle weiteren Daten werden spätestens nach 21 Tagen gelöscht. Ein Löschgesuch müsste nach Art. 12 Abs. 3 DSGVO spätestens nach einem Monat beantwortet werden. Das Löschgesuch wäre bei Fristablauf bereits obsolet.</p> <p>✓ Eine Überprüfung der automatisierten Entscheidungsfindung (Überprüfung der Empfehlungen im Kontaktfall im Rahmen der Phase 3.2) nach Art. 22 Abs. 3 DSGVO ist nicht notwendig, da durch die App keine rechtsverbindlichen Entscheidungen getroffen werden, sondern nur Empfehlungen ausgesprochen werden.</p>	

9. Löschung/ Speicherbegrenzung

Dem Datenschutzziel der Datenminimierung folgend, dürfen personenbezogene Daten nur solange verarbeitet werden, wie dies zur Zweckerreichung notwendig ist. Nachfolgend werden Designentscheidungen dargestellt, die die Speicherbegrenzung umsetzen.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Gefahr von Deanonymisierungsangriffen</p> <p>Sollten die Daten nicht nach 14 Tagen gelöscht werden, wäre es möglich, sie auch rückwirkend mit anderen Daten in Verbindung zu bringen sowie Deanonymisierungsangriffe zu verüben.</p>	D-9-1		<ul style="list-style-type: none"> ✓ Die Positivschlüssel werden vom CWA Server gelöscht sobald sie einen Zeitraum betreffen, der länger als 14 Tage zurückliegt. ✓ Die durch die CWA App berechneten Risikowerte werden, bis zur Neuberechnung aber bis zu maximal 2 Wochen gespeichert und dann gelöscht. 	<p>Solution Architecture.md – GitHub DSK CWA App, 7.4</p>
	D-9-3		<ul style="list-style-type: none"> ✓ Der QR-Code/GUID wird nach dem Pairing des mobilen Endgerätes in der CWA App gelöscht. 	DSK CWA App, 7.4
	D-9-4		<ul style="list-style-type: none"> ✓ Alle Daten werden vom Verification Server nach 21 Tagen gelöscht. 	<p>Software Design Verification Server DSK Verifikation und Testergebnis, 6.1.6</p>
	D-9-5		<ul style="list-style-type: none"> ✓ Löschung von Schnelltests 	DSK CWA App, v2.1 7.4.15.2

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>Die CWA App erlaubt es dem CWA-Nutzer (PCR-/ Schnell-) Tests manuell aus der CWA App zu löschen.</p> <p>Beim Löschen eines Schnelltests sollen alle Attribute in der Datenstruktur für den aktuellen Schnelltest Test zurückgesetzt werden.</p> <p>⚠ Zugehörige Einträge im Kontakt Tagebuch sollen nicht gelöscht werden.</p> <p>✓ Die Löschung eines Schnelltests wird durch jede der folgenden Faktoren ausgelöst:</p> <ul style="list-style-type: none"> • manuell, wenn der Benutzer den Schnelltest löscht • wenn der CWA-Nutzer die Funktion zum Zurücksetzen in der App nutzt (siehe sogleich) <p>⚠ Ein Antigen Schnelltest wird nicht von der CWA App automatisch gelöscht.</p> <p>✓ Die Löschung der Schnelltest auf dem TestResult Server erfolgt nach 21 Tagen.</p>	
	D-9-5a		Löschen der Schnelltestprofile	DSK_CWA-App v2.2, 7.4.15

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>Neben den Metadaten zu den Schnelltests werden auch die Daten für das Schnelltest-Profil in der CWA App gespeichert. In der CWA App gibt es nur ein Schnelltest-Profil. Es ist nicht möglich mehrere Schnelltest-Profile in der CWA App zu hinterlegen. Die Verwaltung der Daten im Schnelltest-Profil erfolgt durch den CWA-Nutzer. Dieser kann sein Schnelltest-Profil jederzeit manuell löschen.</p>	
	D-9-5b		<p>Löschung von Impfzertifikaten/ Testzertifikaten</p> <p>Bei der Nutzung der Impfzertifikat-Funktion werden Daten aus den Impfzertifikaten in der CWA App gespeichert. Der CWA-Nutzer kann diese entweder durch eine manuelle Löschung (über den Detail-Screen des jeweiligen Impfzertifikates) aus der CWA App entfernen oder der CWA-Nutzer kann die Daten über die InApp-Reset-Funktion löschen.</p>	DSK CWA App v2.3, 7.4.18, DSK CWA App v2.4, 7.4.19
	D-9-5c	Art. 10 Abs. 3 DCC-I-VO	<p>Löschung von personenbezogenen Daten auf dem DCC-Server (im Zusammenhang mit Testzertifikat)</p> <p>Art. 10 Abs. 4 DCC-VO bestimmt, dass die zur Ausstellung verwendeten personenbezogenen Daten nicht länger gespeichert werden dürfen, als das COVID-Zertifikat selbst gültig ist. Dies wird umgesetzt.</p>	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
	D-9-5d		<p>Löschen von Daten zum Genesenzertifikat</p> <p>⚠ Die Daten zum Genesenzertifikat werden nicht von der CWA App durch eine automatische Löschroutine aus der CWA App gelöscht. Sofern der CWA-Nutzer die Daten zu einem Genesenzertifikat aus der CWA App entfernen möchte, kann er dies entweder über eine manuelle Löschung vollziehen oder er nutzt die InApp-Reset Funktion. Zur Löschung der Daten über die manuelle Löschung, muss der CWA-Nutzer über die Tab-Navigation zu den Zertifikaten wechseln. Dort kann er das zu löschende Zertifikat auswählen und unter den Details des Zertifikat findet der CWA-Nutzer den Button zur Löschung des Zertifikats aus der CWA App.</p>	DSK CWA App v2.5, 7.4.21
	D-9-5e		<p>Löschen von Daten zu Familienzertifikaten</p> <p>⚠ In der CWA App findet keine automatische Löschung der Daten statt. Sofern der CWA-Nutzer die Daten aus seiner CWA App entfernen möchte, kann dieser die entsprechenden Zertifikate manuell löschen oder der CWA-Nutzer nutzt die InApp-Reset Funktion.</p>	DSK CWA App v2.5, 7.4.22

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>⚠ Andere Personen, deren Zertifikate vom CWA-Nutzer eingescannt wurden, können eine Löschung nur über den CWA-Nutzer erreichen.</p>	
	D-9-6		<p>✓ Die Deinstallation der App bewirkt die Löschung aller lokal in der CWA App erhobenen Daten.</p>	DSK CWA App 7.4
	D-9-7		<p>✓ Alle Daten werden vom Test Result Server nach 21 Tagen gelöscht (maßgeblich ist das Datum aus dem Datenfeld „result_date“). Es werden alle Daten gelöscht deren „result_date“ älter als 21 Tage ist.</p>	Software Design Test Result Server DSK Verifikation und Testergebnis, 6.2.6
End-of-Live-Verhalten der CWA-App	D-9-9		<p>Nachdem ein CWA-Nutzer seine Positivschlüssel geteilt hatte, war die App nur in einem eingeschränkten Umfang weiter nutzbar, da ursprünglich angenommen wurde, dass eine weitere Nutzung der CWA App nach einer Corona-Infektion möglicherweise nicht mehr nötig sein könnte. Der CWA-Nutzer konnte die CWA App aber auch bisher schon weiter nutzen, indem er einen Factory-Reset oder eine Neuinstallation durchgeführt hat.</p>	DSK_CWA-App v1.13, Kap. 6.9

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>Mit Version 1.13 wurde dem CWA-Nutzer ermöglicht, die App im gewohnten Umfang weiter zu nutzen, auch wenn eine bestätigte Corona-Infektion vorlag und er seine Positivschlüssel geteilt hatte.</p> <p>Deshalb wurde mit Release 1.13 der CWA App das „End-of-Life“ Verhalten optimiert. Der CWA-Nutzer kann jetzt sehr einfach mittels eines Buttons auf dem Home-Screen die Risikoberechnung wieder einschalten und die CWA App im gewohnten Umfang weiter nutzen.</p>	

10. Trennungskontrolle

Im nachfolgenden Kapitel werden Designentscheidungen aufgeführt, die der der Trennungskontrolle dienen. Die Trennungskontrolle dient ebenfalls dem Schutzziel der Zweckbindung/ Nichtverkettung.

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Trennungskontrolle</p> <p>Hierbei handelt es sich um Maßnahmen, welche gewährleisten, dass zu</p>	D-10-1		<p>✓ Es erfolgt bei einer evtl. Programmentwicklung eine Funktionstrennung zwischen Test- und Produktionsumgebung.</p>	DSFA Bericht, Anhang TOMs, Ziff. 1045, 1069

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische oder physikalische Trennung der Daten erreicht werden.				
	D-10-2		✓ Es dürfen nur solche Daten erhoben, gespeichert oder verarbeitet werden, die unmittelbar dem eigentlichen Zweck dienen, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses zwingend notwendig sind. Dieser Zweck darf sich in keinem nachgelagerten Schritt der Verarbeitung, auch nicht nach einer Übermittlung ändern.	DSFA Bericht, Anhang TOMs, Ziff. 1065
	D-10-3		✓ Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit unterschiedlichen Vertragszwecken sind zu dokumentieren und anzuwenden.	DSFA Bericht, Anhang TOMs, Ziff. 1066
	D-10-4		✓ Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit	DSFA Bericht, Anhang TOMs, Ziff. 1066

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>unterschiedlichen Vertragszwecken sind zu dokumentieren und anzuwenden.</p>	
	D-10-5		<p>✓ Die Testergebnisse werden nicht auf dem Verification Server, sondern nur auf dem Test Result Server gespeichert. Die Daten werden auf dem Verification Server, Test Result Server und Portal Server getrennt voneinander verarbeitet.</p>	DSFA Bericht, Anhang TOMs, Ziff. 1067
Trennung PCR-Test und Schnelltest	D-10-6		<p>Registrierung eines Schnelltests</p> <p>Beim Scannen eines QR-Codes überprüft die CWA App die erfassten Daten. Aus den Daten kann abgelesen werden, ob es sich um einen QR-Code zum Registrieren eines Schnelltests oder einen PCR-Tests handelt.</p> <p>Sofern es sich bei dem eingescannten QR-Code um einen Antigen Schnelltest handelt, wird dieser wie folgt evaluiert und verarbeitet:</p> <ol style="list-style-type: none"> 1. QR-Code einlesen: Beim Einlesen des QR-Codes werden die in base64url-kodierten Daten ausgelesen und in eine Datenstruktur überführt. Diese ermöglicht es auf die verschiedenen Daten zuzugreifen. Sofern es nicht möglich ist die notwendigen Daten aus den eingescannten Daten zu extrahieren, schlägt das Scannen des QR-Codes 	DSK CWA App v2.1, 7.4.15.1

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>fehl, und dem Benutzer wird eine Fehlermeldung angezeigt.</p> <p>2. Validierung der QR-Code-Attribute; Sofern bei der Validierung ein Fehler auftritt, wird der QR-Code als ungültig angesehen und dem CWA-Nutzer wird eine Fehlermeldung auf dem Screen angezeigt.</p> <p>3. Registrierungs-Token abrufen: Senden einer Anfrage an den Verifizierungsserver, um ein RT - Registration Token für den Hash des GUID zu erhalten.</p> <p>4. Ab diesem Punkt fragt die CWA App in bestimmten Abständen den CWA Verifikationsserver an, ob das Ergebnis für den eingescannten QR-Code vorliegt. Sofern dies der Fall ist, lädt die CWA App sich das Ergebnis herunter und zeigt dem CWA-Nutzer dies an.</p>	
<p>Authentifizierung der PoC für die Übermittlung von Antigen-Schnelltestergebnissen</p>	<p>D-10-7</p>		<p>Die PoC Rest API prüft das Testergebnis auf Einhaltung des für Antigentestergebnisse reservierten Wertebereichs (siehe oben). Im Erfolgsfall überträgt die POC REST API das Testergebnis an den Test Result Server, von welchem das Testergebnis durch die CWA App abgerufen werden kann.</p>	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
			<p>Die Wertebereiche bleiben erhalten, sodass eine logische Trennung im CWA – Backend erfolgt, die eine differenzierte Verarbeitung ermöglicht.</p> <ul style="list-style-type: none"> ✓ Die PoC verbinden sich mit dem PoC-Backend und autorisieren sich diesem gegenüber. ✓ Die Authentisierung durch die PoC-Backend erfolgt mittels mTLS. ✓ Für die Authentifizierung wird ein Zertifikat zur Verfügung gestellt. 	

11. Vertragsverhältnisse

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Einhaltung des Datenschutzes durch Dienstleister und Partner (PoC)</p> <p>Verantwortlicher für die CWA App ist die Bundesrepublik Deutschland, vertreten</p>	D-11-1		<p>Abschluss von Auftragsverarbeitungsverträgen</p> <ul style="list-style-type: none"> ✓ Die Einhaltung der datenschutzrechtlichen Bestimmungen wird durch den Abschluss von 	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>durch das Bundesministerium für Gesundheit, vertreten durch das Robert Koch-Institut (RKI).</p> <p>Vertragspartner des RKI sind:</p> <ul style="list-style-type: none"> • Google und Apple (für die Bereitstellung der App in den App Stores und die Bereitstellung des Exposure Notification Frameworks (ENF)). <p>Das RKI bedient sich als Verantwortlicher für den Betrieb der CWA App verschiedener Dienstleister. Direkte Unterauftragnehmer des RKI sind:</p> <ul style="list-style-type: none"> • T-Systems International GmbH (für den Betrieb des CWA Backends in der Open Telekom Cloud (OTC) und der Hotline), • SAP SE Deutschland (für den 3rd-Level-Support der CWA App), <p>Die weiteren Vertragsverhältnisse, insbesondere die Unterauftragsverhältnisse,</p>			<p>Auftragsverarbeitungsverträgen (nach Art. 28 DSGVO) mit den Dienstleistern sichergestellt.</p> <p>Abschluss von Partnerschaftsverträgen mit den PoC</p> <ul style="list-style-type: none"> ✓ Die PoC werden vertraglich gebunden, um eine sichere und datenschutzkonforme Übertragung von Schnelltestergebnissen in die CWA zu gewährleisten. <p>Dies gilt sowohl für die Portallösung als auch die Anbindung von Drittanbietersystemen über die Antigen-Schnelltest-Schnittstelle.</p>	

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>sind in den Designentscheidungen a.) (D-11-1 aufgeführt und werden dort gepflegt).</p> <p>Für die Anbindung an das System der Corona Warn App zur Übertragung von Testergebnissen aus Antigentests, werden von der TSI Partnerschaftsverträge mit den PoC abgeschlossen.</p> <p>Es muss sichergestellt werden, dass auch die Vertragspartner die datenschutzrechtlichen Bestimmungen einhalten.</p>				
<p>Wahrung der Betroffenenrechte</p> <p>Die Wahrung der Betroffenenrechte könnte gefährdet sein, wenn die Vertragspartner des RKI bei der Wahrung der Betroffenenrechte, beispielsweise den Auskunftspflichten, nicht kooperieren. Dem Benutzer wird durch die Datenschutzhinweise der CWA App transparent gemacht, dass die Datenverarbeitungen durch das Exposure Notification Framework von Google und Apple verantwortet werden.</p>	D-11-2		<p>Vertragliche Regelungen</p> <p>✓ Die Auftragsverarbeitungsverträge mit den Unterauftragnehmern enthalten Regelungen wonach die Vertragspartner zur Kooperation verpflichtet sind.</p>	

II. Bedrohungen durch Hacker, Trolle, Stalker und Einzelpersonen (STRIDE)

Das folgende Kapitel erläutert auszugsweise, welche Sicherheitsbedrohungen erkannt wurden und durch welche Maßnahmen den Sicherheitsrisiken durch Designentscheidungen bei der Entwicklung der CWA App begegnet wurde. Schutzziele der IT-Sicherheit sind die Vertraulichkeit, Integrität und Verfügbarkeit. Die Vertraulichkeit schützt, dass nur berechtigte Personen Zugriff auf die Daten haben. Authentizität und Integrität schützen, dass der Empfänger sicher sein kann, dass die Informationen tatsächlich von dem Absender stammen, von dem er glaubt, sie erhalten zu haben (Authentizität, z.B. gesendete E-Mail oder gespeicherte Datei) und die Daten nicht zwischenzeitlich durch einen Dritten verändert wurden (Integrität). Verfügbarkeit schützt, dass jederzeit auf die Daten zugegriffen werden kann. Im Rahmen des Releasezyklus 2.1 wurde ein ThreatModelling Workshop durchgeführt, der diese Methode berücksichtigt.

Das Kapitel ist entsprechend der Threat Modeling Methode STRIDE aufgebaut. Threat Modeling ist eine Methode, durch die potenzielle Bedrohungen, wie z.B. strukturelle Schwachstellen oder das Fehlen geeigneter Schutzmaßnahmen, identifiziert, aufgezählt und die Prioritäten für Abhilfemaßnahmen festgelegt werden können. Das Threat Modeling beantwortet Fragen wie: "Wo bin ich am anfälligsten für Angriffe? Was sind die relevantesten Bedrohungen? Was muss ich tun, um mich gegen diese Bedrohungen zu schützen?"

Eine Methode für das Threat Modeling ist die sogenannte STRIDE Methode. Diese ordnet die Bedrohung sechs verschiedenen Kategorien zu. Dabei steht jeder Buchstabe der Methode für eine Bedrohung:

S – Spoofing (Angreifer verschleiert seine Identität; Schutzziel: Authentizität)

T – Tampering (Angreifer verändert Daten; Schutzziel: Integrität)

R – Repudiation (Angreifer bestreitet Identität; Schutzziel: Nichtabstreitbarkeit)

I – Information Disclosure (Angreifer verursacht Datenleck; Schutzziel: Vertraulichkeit)

D – Denial of Service (Angreifer überlastet das System mutwillig; Schutzziel: Verfügbarkeit)

E – Elevation of Privilege (Angreifer weitet seine Rechte aus; Schutzziel Authentizität)

1. Spoofing (Identität verschleiern)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
<p>Missbräuchliche Verwendung des QR-Codes</p> <p>Wie bereits oben beschrieben erhält der Benutzer bei der Durchführung des Schnelltests einen QR-Code, den er mit seinem mobilen Gerät einscannen kann. Nach dem Scan besteht die Möglichkeit, das Testergebnis mit der CWA App abzurufen. Soweit ein positives Testergebnis in der Datenbank mit der in dem QR-Code enthaltenen ID verknüpft ist, kann der Benutzer außerdem seine Positivschlüssel der letzten 2 Wochen der Gemeinschaft zur Verfügung zu stellen.</p>	B-1-1		<p>Austausch des QR-Codes gegen neue ID</p> <p>✓ Um dem zu begegnen, wird von der CWA App unmittelbar nach dem Scannen des QR-Codes der QR-Code auf dem Verification Server gegen einen sogenannten Registration Token eingetauscht und der QR-Code auf dem Server als verbraucht gekennzeichnet. Mit dem Registration Token authentifiziert sich die CWA App fortan gegenüber dem Server. Damit kann das Testergebnis nunmehr nur noch mit dem mobilen Gerät abgefragt werden, mit dem der QR-Code gescannt wurde.</p>	DSK CWA App, 4.3

2. Tampering (Daten verändern)

Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Verhinderung des Einspielens falscher Datenpakete	B-2-1		Einsatz von Hash - Funktionen ✓ Um die Integrität der Datenpakete auf QR Codes und um das Bereitstellen gefälschter Inhalte durch andere zu verhindern, werden die Datenpakete im QR code gehasht und vom Client verifiziert.	

3. Repudiation (Abstreiten) - keine Besonderheiten für PoC-Anbindung und Nachweisfunktion

4. Information Disclosure (Datenleck) - keine Besonderheiten für PoC-Anbindung und Nachweisfunktion

5. Denial of Service (Mutwillige Überlastung) – keine Besonderheiten für PoC-Anbindung und Nachweisfunktion

6. Elevation of Privilege (Ausweiten der Rechte) - keine Besonderheiten für PoC-Anbindung und Nachweisfunktion