Datenschutzfolgenabschätzung (DSFA)
VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)

				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
	4	**1) Unbefugte oder unrechtmäßige Verarbeitung durch CWA**																		
R4- Testcenter	5	Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitungen	Zweck und Mittel der Datenverarbeitung werden nicht vom Verantwortlichen bestimmt. Durch die Datenverarbeitung in den Testcentren/ PoC (eigene Verantwortliche) besteht das Risiko, dass durch sie Datenverarbeitungen durchgeführt werden, die über ihre Verantwortung hinausgehen bzw. Datenübermittlungen an die CWA-Infrastruktur erfolgen, für die die PoCs verantwortlich sind.	Ja	2	4	4	1	1	1	1	4	4	4	8	RM, DM, VT, IG, IV, TR, ZB	Vertragliche Regelungen mit PoC, Leistungsbeschreibungen für Portal-Anbindung und Antigen-Schnelltest-Schnittstelle			akzeptabel mit Evaluation
R8- Behörden	6	[Release 2.15] Unklare Verantwortlichkeiten in Bezug auf die Datenverarbeitungen	Die Trennung der Verantwortlichkeiten für die verschiedenen Prozessschritte/ Datenverarbeitungen im Zusammenhang mit dem Validierungsservice und dessen Integration in die CWA könnte dazu führen, dass die Betroffenen ihre Rechte nicht durchsetzen können.	Ja	2	0	0	0	0	1	0	2	2	2	4	IV, TR, ZB	Verantwortlichkeiten werden für den CWA Nutzer transparent. Regelungen für Validierungsservices durch BMG in Planung.			akzeptabel
R8- Behörden	7	Fehlende Rechtsgrundlage für den Widerruf von Zertifikaten in der CWA anhand eines "Gruppen Identifiers" (z.B. AusstellerID)	Mit dem Hotfix zur Widerrufsfunktion können Zertifikate in der CWA App als ungültig angezeigt werden, die von einem Arzt, Apotheker oder Impfzentrum ausgegeben wurden, welcher/s u.U. auch personenbeziehbar auf einer Widerrufsliste steht. Es besteht das rechtliche Risiko, dass eine Rechtsgrundlage für	Ja	3	4	4	4	3	1	1	4	4	4	12	DM, VT, IG, VF, IV, TR, ZB	Die Prüfung der Rechtsgrundlage und der erforderlichen Abwägungen erfolgt in Verantwortung der verantwortlichen Stelle. Zum Zeitpunkt des DSFA-Risikoworkshops und der Dokumentation ist diese Prüfung noch nicht abgeschlossen.		rechtliches Risiko, Übernahme durch verantwortliche Stelle und Weisung an die DL	bedingt akzeptabel
R8- Behörden	8	Fehlende Rechtsgrundlage für den Widerruf von gültigen Zertifikaten in der CWA	Mit dem Hotfix zur Widerrufsfunktion implementierten Lösung besteht das Risiko, dass gültige Zertifikate, die von einem blockierten Aussteller ausgestellt wurden, in der CWA App als ungültig angezeigt werden, obwohl diese eigentlich gültig sind.	Ja	3	4	4	4	3	1	1	4	4	4	12	DM, VT, IG, VF, IV, TR, ZB	Die Prüfung der Rechtsgrundlage und der erforderlichen Abwägungen erfolgt in Verantwortung der verantwortlichen Stelle. Zum Zeitpunkt des DSFA-Risikoworkshops und der Dokumentation ist diese Prüfung noch nicht abgeschlossen.		rechtliches Risiko, Übernahme durch verantwortliche Stelle und Weisung an die DL	bedingt akzeptabel
R8- Behörden	9	Fehlende Rechtsgrundlage zur Datenübermittlung von den Testcentren in die CWA-Infrastruktur		Ja	2	4	4	4	1	1	1	4	4	4	8	RM, DM, VT, IG, IV, TR, ZB	Einwilligung wird für diese Funktionen / Verarbeitungstätigkeiten durch die PoC eingeholt (siehe Designentscheidungen c. D-2-2c)			akzeptabel mit Evaluation
R8- Behörden	10	[Release 2.15] Fehlende Rechtsgrundlage für die Datenübermittlung von CWA App zum Validation Service / Inkonstistenzen im Einwilligungstext	Der QR-Code vom Leistungsanbieter enthält einen Parameter, der einen „Einverständnis-Text" (nach der Richtlinie vom eHealth-Network [https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_traveller-onlinebooking_en.pdf] enthält. Nach der Richtlinie soll dieser Parameter dem Wallet-Nutzer (hier CWA-Nutzer) angezeigt werden. In der CWA App wird allerdings ein statischer Text zur Datenverarbeitung angezeigt. Sofern ein Leistungsanbieter einen abweichenden Text zu dem angezeigten Text in der CWA App anzeigt, kann dies zu Reputationsschäden für die CWA Lösung führen und zudem auch noch weitreichende Folgen für die Nutzer der CWA App haben.	Ja	3	3	0	0	0	0	0	1	3	3	9	RM, DM, ZB	Erstellung passender Einwilligungstexte durch die jeweils Verantwortlichen.			akzeptabel mit Evaluation
R1-CWA-Nutzer	11	Datenverarbeitungen nach widerrufener Einwilligung in die Datenübermittlung von den Testcentren in die CWA-Infrastruktur	Ein Nutzer kann sich zu jedem Zeitpunkt dazu entscheiden, die Einwilligung zum Teilen der Daten zu widerrufen. Nach der Übertragung der Daten von den Poc an die CWA (Test Result Server) gibt es keine Möglichkeit, eine Zuordnung zwischen dem Nutzer und den von ihm bereitgestellten Daten herzustellen.	Ja	1	4	4	4	4	4	0	4	0	4	4	RM, DM, VT, IG, IV, TR, ZB	siehe Designentscheidungen a.) (D-2.1-2 (Install), D-2.1-6 (Upload) + Designentscheidung D-3.1-1 + Designentscheidung a.) (Widerruf) D-3.1-8			akzeptabel
R4- Testcenter	12	Unwirksame Einwilligung durch fehlende Freiwilligkeit ("erzwungene Einwilligung") /erzwungene Freiwilligkeit		Ja	1	4	4	1	1	1	1	4	1	4	4	DM, VT, IV, ZB	Vertragliche Regelungen mit PoC, Vorsehen einer Einwilligungslösung (Check-Box) für Portallösung, Muster für Drittanbieter (Antigen-Schnelltest-Schnittstelle), Hinweis auf Freiwilligkeit im Rahmen von Datenschutzinformationen PoC und in der CWA-App.			akzeptabel
R1-CWA-Nutzer	13	Unwirksame Einwilligung aufgrund fehlender/ fehlerhafter ausdrücklicher Einwilligungserklärung (technischer Einwilligungs-Akt)	Die Einholung der Einwilligung erfolgt durch die PoC, daher mittels eines Portals oder durch Schnelltest-Drittanbietet, mittels deren Testcenter-Software bzw. auf anderem Wege.	Ja	1	4	4	1	1	1	1	4	4	4	4	DM, VT, IV, TR, ZB	siehe Designentscheidungen D-2-2c			akzeptabel
R1-CWA-Nutzer	14	Unwirksame Einwilligung aufgrund fehlender Information zu Umfang und Folgen der Schnelltest-Anbindung und Nachweisfunktion + Schnelltest-Profil (CWA-Version 2.2)	Lücken in der Information über die Datenverarbeitung könnten zur Unwirksamkeit der Einwilligungserklärung insgesamt führen. Nutzer könnten durch fehlende Informationen die Schnelltestanzeigen gegenüber Dritten offenbaren, weil ihnen nicht bewusst ist, dass sie dazu nicht verpflichtet sind. Vor allem	Ja	2	4	4	1	1	1	1	4	4	4	8	DM, VT, IV, TR, ZB	Datenschutzinformationen liegen vor, siehe Designentscheidung c. D-4-4			akzeptabel mit Evaluation und ggf. Anpassung der Datenschutzerklärung
R1-CWA-Nutzer	15	Unwirksame Einwilligung aufgrund Nichterreichbarkeit der notwendigen Informationen (sprachliche Barrieren, fehlendes Technikverständnis)	Risiko umfasst auch die unwirksame Einwilligung in Erstellung des Schnelltest-Profils (CWA Version 2.2)	Ja	2	4	4	1	1	1	1	4	4	4	8	DM, VT, IV, TR, ZB	Datenschutzinformationen in leichter Sprache formuliert, Übersetzungen liegen vor.			akzeptabel, mit Evaluation und ggf. Anpassung der Datenschutzerklärung
R1-CWA-Nutzer	16	Unbefugte Nutzung der Funktionen durch Minderjährige unter 16 Jahre	Minderjährige könnten in den Testcentren ihre Einwilligung erteilen, ohne dass diese etwa die Datenübermittlung an die CWA ab- und einschätzen könnten. Dritte könnten sich negative Testergebnisse auch von Minderjährigen anzeigen lassen (etwa in Schule, Verein). Release 2.15: MJ könnten die Funktionen zur Validierung von Zertifikaten nutzen, ohne dass diese die Datenverarbeitungsprozesse und die verschiedenen Verantwortlichkeiten ab- und einschätzen könnten.	Ja	3	3	3	3	1	1	1	3	3	3	9	DM, VT,IG, IV, TR, ZB	Siehe Designentscheidungen a. D-3.1-2, eine Altersabfrage erfolgt im Rahmen der CWA nicht; die Auswertemöglichkeiten des RKI und Rückschluss auf Minderjährige sind nicht möglich // Eine Altersabfrage erfolgt durch die PoC. Es ergeht der Hinweis, dass Minderjährige, die Nutzung der CWA mit ihren Erziehungsberechtigten besprechen sollen.		Verhältnismäßigkeit Restrisiko ist generell bewertet (siehe DSFA-Bericht), Folge des Verzichts auf Erhebung von Altersangabe und weiterer Daten	bedingt akzeptabel
R4- Betreiber Server (T)	17	Abhängigkeiten von Dienstleistern/ Software- und Firmware Hersteller (Ausfall externer Dienstleistern)	Bei einem Ausfall des Dienstleisters könnten sowohl die PoC als auch die CWA nicht mehr betrieben werden. Der Dienst (Schnelltest-Anbindung und Anzeigefunktion) wäre nicht verfügbar und die Nutzung wäre eingeschränkt.	Ja	2	0	0	0	2	0	2	2	3	2	6	VF, TR	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen D-11-1).			akzeptabel, mit Evaluation
R4- Testcenter	18	Fehlende/ unzureichende vertragliche Regelungen mit Point-of-Care (PoC)	Soweit die Systemintegration der PoC nicht rechtmäßig, zweckgebunden, datenschutzkonform und IT-sicher ist, entstehen Risiken für CWA-Nutzer.	Ja	2	3	3	3	3	0	2	2	3	3	6	ZB , TR	Partnerverträge und Leistungsbeschreibung mit PoC, siehe Designentscheidungen c.) D-3.1-2.			akzeptabel, mit Evaluation
R4- Betreiber Server (T)	19	Fehlende, unzureichende vertragliche Regelungen mit Dienstleistern (Auftragsverarbeitung/ Vertrag zur gemeinsamen Verantwortung) - mit T/SAP	Fehlende Vertragsanpassungen mit T/SAP könnten zu Lücken in der Gewährleistung der Sicherheit der Verarbeitung führen, da durch die Anbindung der Testcenter personenbezogene Daten als Klardaten verarbeitet werden, obwohl die bisherigen Verträge/ TOM lediglich von einer Verarbeitung von Pseudonymen ausgehen.	Ja	1	3	3	3	3	0	2	2	3	3	3	ZB, TR	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen a. D-11-1).			akzeptabel
R4- Betreiber Server (T)	20	Identifizierung der Nutzer (direkte Identifizierung) auf CWA-Komponenten	Nicht-pseudonymisierte personenbezogene Daten liegen nur auf dem Schnelltest-PoC-Backend. In die CWA-Infrastruktur (zu Testresult-Server) werden nur das Testergebnis und Hash (CWA Test ID) übertragen.	Ja	1	1	4	1	1	1	1	1	1	1	4	DM	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen a. D-11-1).			akzeptabel
R4- Testcenter	21	Erhebung und Speicherung nicht-notwendiger Daten, inklusive Nutzer- und Metadaten durch Testcenter	Durch die Testcenter könnten Nutzer- und Metadaten gespeichert werden, die zur Identifikation von CWA-Nutzern/ PoC-Mitarbeitern genutzt werden könnten.	Ja	3	4	4	0	0	0	0	2	0	4	12	DM, IG, ZB	Die Einwilligung der CWA-Nutzer ist erforderlich. Datenverarbeitung in Verantwortung der PoCs; Leistungsbeschreibungen & zusätzliche Bedingungen für PoC vorhanden.		Technische Maßnahmen außerhalb der CWA Verantwortung. Vertragliche Verpflichtung der PoC // Harte Mitwirkungspflichten und Sanktion/ außerordentliche Kündigung.	bedingt akzeptabel
R4- Betreiber Server (T)	22	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Betreiber CWA (Backend)	Durch die Betreiber der CWA könnten - über die Schnittstellen zu den PoC - Nutzer- und Metadaten gespeichert werden, die zur Indentifikation von CWA-Nutzern oder PoC-Mitarbeitern genutzt werden könnten.	Ja	2	4	4	0	0	0	0	2	0	4	8	DM, IG, ZB	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen a.) D-11-1) + Designentscheidungen c (Die pseudonymen Daten werden (auch durch die PoC) in die CWA verschlüsselt übertragen und verschlüsselt gespeichert).			akzeptabel mit Evaluation
R10 - Validation Service Provider/ Leistungsanbieter	23	[Release 2.15] Speicherung von personenbezogenen Daten außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA	Es besteht die Möglichkeit, dass personenbezogene Daten außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA gespeichert werden.	Ja	3	3	3	0	0	0	0	3	3	3	9	DM, VT, IV, TR, ZB	Keine Mitigationsmaßnahmen in der CWA .			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	24	Erhebung und Speicherung nicht-notwendiger Daten, inkl. Metadaten (TK-Daten) durch Entwickler CWA (SAP)	In der CWA könnten Daten gespeichert werden, die den Entwicklern eine Identifikation der CWA-Nutzer erlauben.	Ja	1	4	4	0	0	0	0	2	0	4	4	DM, IG, ZB	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen D-11-1).			akzeptabel
	25	**2) Verarbeitung wider Treu und Glauben**																		

Datenschutzfolgenabschätzung (DSFA)
VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)

				Risikobewertung															
						Schadensausmaß													
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R4- Betreiber Server (T)	26	Auftreten von Sicherheitslücken und Datenschutzvorfällen bei App-Entwickler und/ oder Serverbetreiber (Vertrauensverlust der Bevölkerung in/ geminderte Vertrauenswürdigkeit der CWA und IT-Infrastruktur).		Ja	1	0	0	0	0	0	0	0	0	3	3	ZB, DSMS/ ISMS	AVV mit DL; Vereinbarung von TOM nach Art. 28 DSGVO (siehe Designentscheidungen D-11-1).			akzeptabel
R4- Testcenter	27	Auftreten von Sicherheitslücken und Datenschutzvorfällen bei den Testcentern (Vertrauensverlust der Bevölkerung in/ geminderte Vertrauenswürdigkeit der CWA und IT-Infrastruktur)	Die Umsetzung der Point-of-Care (PoC) Lösung liegt nicht im Verantwortungs-/Zuständigkeitsbereich der CWA Lösung. Aus diesem Grund gibt es auch keine Möglichkeit, die Sicherheits-/Datenschutzkonzepte der PoC Lösung zu prüfen und/oder zu validieren. Daher könnten „Datenleck-" Risiken durch das CWA Team nicht mitigiert werden. Dies gilt umso mehr, als Drittanbieter (mittels API) an das System angeschlossen werden können.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB, DSMS/ ISMS	Die Umsetzung der Security-/ DPP-/ Compliance-Vorgaben für die PoC-Lösung sollte externe geprüft und bewertet werden, um Probleme im Kontext der CWA-Lösung vermeiden zu können. Verträge (Leistungsbeschreibungen) mit den PoC werden abgeschlossen und enthalten z.B. die Verpflichtung, Missbräuche zu verhindern, Zugangsdaten geheim zu halten und bei der Aufklärung von Sicherheitsvorfällen zu unterstützen.			akzeptabel mit Evaluation
R8- Behörden	28	Überraschende negative Datenverarbeitung durch Widerruf von Zertifikaten	Sofern sich ein CWA-Nutzer auf die korrekte Anzeige der Gültigkeit der DCC Zertifikate verlässt, kann der spontane Widerruf von DCC Zertifikaten zu erheblichen Problemen und Nachteilen für den Nutzer führen. Z.B. kann dieser eine geplante Reise nicht antreten oder eine geplante Veranstaltung nicht besuchen.	Ja	2	1	3	3	2	1	1	3	3	2	6	VT, IG, TR, IV	Per Benachrichtigung werden die CWA-Nutzer vorab darüber informiert, dass ihr Zertifikat möglicherweise widerrufen wird und dass sie die Möglichkeit haben, sich ein neues ausstellen zu lassen.			akzeptabel mit Evaluation
	29	**3) Für die Betroffenen intransparente Verarbeitung**																	
R8- Behörden	30	Unvollständige, unverständliche Datenschutzinformationen für die weiteren Funktionalitäten der CWA (Schnelltest-Anbindung + Anzeige)		Ja	1	2	2	2	0	0	0	3	4	4	4	TR, ZB	Datenschutzinformationen vorhanden. Siehe Designentscheidungen c.) D-4-4.			akzeptabel
R4- Betreiber Server (T)	31	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten mittels der Server und Komponenten in der OTC		Ja	3	0	0	0	0	0	0	2	3	1	9	TR, ZB	Datenschutzinformationen und Informationen auf GitHub und AV-Vertrag mit SAP/ T.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	32	Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten und Funktionsweise der CWA		Ja	2	0	0	0	0	0	0	2	3	1	6	T R	Datenschutzinformationen und Informationen auf GitHub und AV-Vertrag mit SAP/ T.			akzeptabel mit Evaluation
R1-CWA-Nutzer	33	[Release 2.15] Gefahr der Intransparenz und fehlenden Prüfbarkeit der verarbeiteten Daten im Zusammenhang mit der Integration des Validation Service	Der CWA Nutzer kann nicht innerhalb der App die Richtigkeit und Rechtmäßigkeit der Datenverarbeitung seiner personenbezogenen Daten außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA nachvollziehen.	Ja	2	1	1	1	0	1	0	1	3	1	6	TR	Durch CWA-Nutzer aktivierbare Event-Logging-Funktion in datenschutz-/rechtskonformer Weise, soweit Datenverarbeitungen innerhalb der CWA betroffen sind. Darüber hinaus wird es einen Hinweis in den FAQ für CWA-Nutzer geben, um die Transparenz der Event-Logs zu erhöhen.			akzeptabel mit Evaluation
R8- Behörden	34	Unvollständige, unverständliche Informationen im Zusammenhang mit dem Widerruf von Zertifikaten	CWA-Nutzern könnte die Widerrufsfunktion, die entsprechende Datenverarbeitung und deren Folgen intransparent sein. Vertrauensverlust in die App oder "Verwirrung" bei der Ausübung von Rechten und Freiheiten, die mit der Nutzung der Zertifikate verbunden sind, könnten die Folge sein. Durch das Ausschalten von Benachrichtigungen könnte der CWA-Nutzer vom Widerruf überrascht werden, mit erheblichen Nachteilen für die Ausübung seiner Rechte.	Ja	2	1	1	1	1	1	1	2	3	1	6	TR	Die Datenschutzinformationen werden ggf. angepasst. Auf den Screens in der CWA-App werden Hinweises auf den Widerruf, Gründe und Folgen angezeigt.		Zusätzlich soll auf die FAQ/ Webseite des RKI verwiesen werden, die die Gründe für den Widerruf für den Betroffenen transparenter machen.	akzeptabel mit Evaluation
	35	**4) Unbefugte Offenlegung von und Zugang zu Daten**																	
R4- Betreiber Server (T)	36	Re-Identifizierung durch Korrelation der erhobenen Daten (+ Publikation)	Auch wenn die Daten bei der Schnelltest-Anbindung grundsätzlich in pseudonymisierter Form übertragen werden, kann nicht ausgeschlossen werden, dass unter speziellen Bedingungen (z.B. einer sehr geringen Anzahl an CWA-Nutzern, die der Nutzung des Features zugestimmt haben und diese auch aktiv nutzen) Rückschlüsse auf einzelne Nutzer (z.B. mögliche Corona-Warnungen, Dauer bis zum Teilen der Schlüssel, ...) möglich werden könnten. Die Offenbarung der CWA-Nutzer kann dazu führen, dass der CWA-Nutzer staatlichen Kontrollmaßnahmen ausgesetzt wird. In einem hypothetischen Scenario, wo SAP/Telekom als Angreifer fungieren, könnten diese die von CWA-Nutzern geteilten Daten nutzen, um diese auf anderen Medien öffentlich zu verbreiten. Dadurch könnte es einem Angreifer möglich sein, anhand neuer, ihm zugänglichen Datenpunkte eine Re-Identifikation von CWA-Nutzer einfacher durchzuführen.	Ja	2	2	2	1	1	1	1	1	1	2	4	DM, VT, ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen a. D-11-1.			akzeptabel
R4- Betreiber Server (T)	37	Offenlegung von personenbezogenen Daten von Mitarbeiter der Schnelltestzentren	Personenbezogenen Daten von PoC Mitarbeiter werden bei der Schnelltest-Portal-Lösung in einem IAM Server im Backend gespeichert. Bei mangelhafter Konfiguration der Server könnten diese Informationen für Dritte oder für anderen Mandanten sichtbar werden. Während der Entwicklung besteht ein Risiko, dass User-Daten des Testers für Support-Mitarbeiter sichtbar sind, die dies nicht zur Aufgabenerledigung brauchen.	Ja	2	1	2	1	1	1	1	1	1	2	4	VT, ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen a, D-11-1, Mandantentrennung im Backend, Berechtigungskonzept und Monitoring /Alerting // Mit Anbindung des UC wird ein Level Switch eingebaut, der es nur den zuständigen Mitarbeitern des Level 3 erlaubt, Zugriff zu nehmen.			akzeptabel
R10 - Validation Service Provider/ Leistungsanbieter	38	[Release 2.15] Offenlegung von personenbezogenen Daten beim Leistungsanbieter	Personenbezogene Daten können beim Leistungsanbieter anfallen und erhoben werden.	Ja	2	3	3	1	0	0	0	1	1	3	6	VT, ZB	Keine Mitigationsmaßnahmen in der CWA.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel mit Evaluation
R2- Hacker	39	[Release 2.15] Offenlegung von personenbezogenen Daten/ Buchungsdaten im Netzverkehr	Personenbezogene Daten können beim Transfer über das Internet vor dem Leistungs- und Validierungsanbieter abgefangen werden.	Ja	3	1	3	1	0	0	0	1	1	3	9	VT, ZB	Keine Mitigationsmaßnahmen in der CWA // CWA - Nutzer müssen ihrerseits IT-Sicherheit sicherstellen und sichere Netzwerkverbindungen initiieren.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel mit Evaluation
R2- Hacker	40	[Release 2.15] Offenlegung von personenbezogenen Daten/ Benutzerdaten gegenüber "falschem Validierungsservice" (durch Man-in-the-Middle Angriff)	Für die Verarbeitung entscheidende Daten können vor oder beim Transfer über das Internet vor dem Leistungs- und Validierungsanbieter abgefangen und modifiziert werden.	Ja	2	1	4	4	1	1	1	1	1	4	8	VT, IG, ZB	Keine Mitigationsmaßnahmen in der CWA.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen. In der App könnte ein Warnhinweis für CWA-Nutzer erteilt werden, die Übertragung der DCCs sowie Zahlungsdaten/ Kreditkartendaten nicht über unsichere Netze durchzuführen (z.B. öffentliche WLAN Netze).		akzeptabel mit Evaluation
R4- Testcenter	41	Unbefugter Zugriff auf Testberichte in PoC (Ausnutzung der Schnittstelle des PoC)	Im PoC gibt es eine Schnittstelle, die es erlaubt, Testberichte mit allen persönlichen Daten von Getesteten (etwa des vergangenen Tages) zu ziehen, um Meldepflichten an das Gesundheitsamt zu erfüllen. Diese Schnittstelle könnte von Mitarbeitern des PoC (über die Aufgabenerfüllung hinaus) missbraucht und somit die Vertraulichkeit verletzt werden.	Ja	3	1	3	1	1	1	1	3	3	3	9	VT, IV, TR, ZB	Gewährleistung der Vertraulichkeit durch PoC (Verantwortung der PoC). Einsatz von Rollen- und Berechtigungskonzepten und technische und organisatorische Zugriffsbeschränkungen.			akzeptabel mit Evaltuation

Datenschutzfolgenabschätzung (DSFA)
VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)

				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R2- Hacker	42	Re-Identifizierung von CWA-Nutzern durch unbefugten Zugriff (Auslesen des QR-Codes bei der personalisierten Übertragung von Schnelltestergebnissen durch Dritte im PoC) oder Erfassung des Schnelltest-Profils	Die personenbezogenen Daten im QR-Code bleiben lesbar. Mit einem QR-Code-Scanner können diese somit unbefugten Dritten gegenüber offenbart werden, wenn sie Zugriff auf den QR-Code erlangen. Dies könnte im PoC erfolgen, wenn die Vertraulichkeit nicht gewahrt wird, etwa indem QR-Codes von Dritten oder CWA-Nutzer ausgedruckt und nicht entsorgt werden oder Dritte die Möglichkeit erlangen, nicht für sie bestimmte QR-Codes zu scannen. Ab CWA [Release 2.2]: Beim Warten an einer Teststation könnte es passieren, dass Schnelltest-Profile von Dritten erfasst werden (z.B. Überwachungskamera, Kamera,….), während der CWA-Nutzer sein Schnelltest-Profil einscannt. Die aufgezeichneten Daten könnten dann durch den Dritten unrechtmäßig weiterverarbeitet werden.	Ja	2	1	3	1	1	1	1	3	3	3	6	VT, TR, IV, ZB	Maßnahmen zur IT-Sicherheit der Verarbeitung durch PoC, Sensibilisierung der PoC-Mitarbeiter.			akzeptabel mit Evaluation
R2- Hacker	43	Re-Identifizierung von CWA-Nutzern durch unbefugten Zugriff (Auslesen des QR-Codes bei der personalisierten Übertragung von Schnelltestergebnissen durch Dritte im CWA-Backend)	In den Fällen der personalisierten Übertragung des Schnelltestergebnisses wird weder der QR-Code, noch personenbezogene Daten an das CWA-Backend weitergeleitet, sondern lediglich die Hash (CWA Test ID). Ein "De-Hashing" mit der Folge der Re-Identifizierung von CWA-Nutzern ist nicht ausgeschlossen, aber nur unter extrem hohen Aufwand möglich.	Ja	1	1	3	1	1	1	1	3	3	3	3	VT, TR, IV, ZB	Einsatz von Hash-Funktionen. Siehe Designentscheidung a.) B-2-1 und Designentscheidungen c.) 5-1-8.			akzeptabel
R1-CWA-Nutzer	44	Re-Identifizierung von CWA-Nutzern/ Offenlegung von Gesundheitsdaten durch unbefugten Zugriff (Auslesen der QR-Code Anzeige bei der personalisierten Übertragung von Schnelltestergebnissen oder Mitlesen der Anzeige von Zertifikatsarten auf dem Smartphone - "Shoulder-Surfing")	Nach dem Scannen sind die personenbezogenen Daten, die bei der personalisierten Übertragung von Schnelltestergebnissen in den QR-Code geschrieben werden, auf dem Smartphone lesbar. Bei der Anzeige auf dem Smartphone könnten diese gegenüber unbefugten Dritten offenbart werden, die Zugriff auf das Smartphone oder Einblick in die Anzeige erhalten. Ebenso kann bei Anzeige von Impf-, Test- und Genesenenzertifikaten durch nahestehende Personen unbefugt Einsicht in den Impf- oder Teststatus einer Person genommen werden bzw. über das Genesenenzertifikat der Rückschluss gezogen werden, dass bereits eine Erkrankung vorlag.	Ja	2	1	3	1	1	1	1	3	3	3	6	VT, TR, IV, ZB	Sensibilisierung der CWA-Nutzer, Dritten keinen Einblick in Anzeigen der App zu erlauben. Nach dem Scannen des QR-Codes im PoC werden die Daten auf dem Smartphone (verschlüsselt in der Sandbox) gespeichert. Mit [Release 2.5] und der Einführung einer weiteren Zertifikatsart (Genesenenzertifikat) wird dem CWA-Nutzer die Auswahl einer datensparsamen Variante der Darstellung des isolierten QR-Codes ermöglicht.			akzeptabel mit Evaluation
R1-CWA-Nutzer	45	[Release 2.15] Offenlegung von Buchungsinformationen und/ oder personenbezogenen/ personenbeziehbaren Informationen über den vom Leistungsanbieter im Anbieter-Buchungssystem angezeigten QR-Code für einen nicht beabsichtigten Empfänger/ Betrachter (Shoulder-Surfing)	Personenbezogene Daten können beim Transfer über den QR-Code vor dem Mobilgerät des CWA-Nutzers abgefangen werden.	Ja	2	1	3	1	0	0	0	1	1	1	6	VT	Keine Mitigationsmaßnahme in der CWA.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel mit Evaluation
R2- Hacker	46	[Release 2.15] Mögliche Offenlegung personenbezogener Daten/ personenbeziehbarer Daten druch das Logging des Init-Tokens	Ein Angreifer, der Zugriff auf das Init-Token erhält, könnte die darin enthaltenen Informationen dazu nutzen, sich Zugang zu weiteren personenbezogenen/ personenbeziehbaren Informationen zu verschaffen.	Ja	2	0	3	0	0	0	0	0	0	1	6	VT		Init-Token aus Logfiles der CWA entfernen (in Prüfung).		
R2- Hacker	47	Re-Identifizierung von Ärzten oder Apothekern, die Zertifikate ausgeben und vom Widerruf betroffen sind (Verteilung Identifier, z.B. AusstellerID, über das CWA-Backend)	Die Identifier (Liste der zu widerrufenden DCC) werden über die App-Konfiguration über den CWA-Server und das CDN an die CWA App weitergeleitet. Nachdem die App-Konfiguration für alle zur Verfügung steht, ist es u.U. möglich, Identifier und die Namen von Ärzten, Apothekern zu ermitteln. Verbindet man diese Information mit anderen Informationen, besteht die Möglichkeit herauszufinden, welcher Aussteller gefälschte Zertifikate (nach Angabe der CWA App) verbreitet hat. Dies könnte zu verschiedenen negativen Folgen für die Aussteller führen; insbesondere auch dann, wenn versehentlich Falschangaben zum Widerruf führen.	Ja	2	1	3	3	1	1	1	1	1	1	6	VT, IG	Technische Mitigation nicht möglich. Re-Identifikationsmöglichkeit ist Folge der gewählten technischen Lösung (AusstellerID als Bestandteil der UVCIs für den Widerruf zu verwenden und in der Config über CDN zu verteilen).			akzeptabel mit Evaluation
R2- Hacker	48	Re-Identifizierung von CWA-Nutzern, die vom Widerruf von Zertifikaten betroffen sind (Verteilung Identifier, z.B. AusstellerID über CWA-Backend)	Bei der mit dem Hotfix eingeführten Widerrufsfunktion werden die Aussteller-IDs nicht zur Verarbeitung als selbstständige Daten übertragen, sondern als ein Bestandteil einer abschließenden Menge von UVCI. Ist die Gruppe der mittels der AusstellerIDs widerrufenen Zertifikate hinreichend klein, ist ein Rückschluss auf den betroffenen CWA-Nutzer nicht auszuschließen.	Ja	2	1	3	3	1	1	1	1	1	1	6	VT, IG	Eine technische Mitigation ist nicht möglich. Re-Identifikationsmöglichkeit ist Folge der gewählten technischen Lösung (AusstellerID als Bestandteil der UVCIs für den Widerruf zu verwenden und in der Config über CDN zu verteilen).			akzeptabel mit Evaluation
R1-CWA-Nutzer	49	Rückschlüsse auf mögliches Reiseverhalten von CWA-Nutzern	Sofern die Anzahl der Corona-Infektionen auf Kreis-/ Bundesland-Ebene sehr gering ist, wäre es möglich, dass sich das Re-Identifikationsrisiko für den CWA-Nutzer durch Auswertung der Statisitiken (Anzahl der Warnungen pro Kreis) in Abhängigkeit von Pandemiegeschehen signifikant erhöht (Neuaufnahme des Risiko mit [Release 2.6)/ Risikobewertung in Anlehnung an vergleichbare Risiken in VT_1_2_4). Einem Angreifer wäre es möglich, gewisse Rückschlüsse auf mögliche Reisepläne eines CWA-Nutzers zu ziehen.	Ja	2	1	3	1	1	1	1	3	3	3	6	Vt, IV, TR, ZB	Keine Mitigationsmaßnahmen [Release 2.6].			akzeptabel mit Evaluation
R9 - DCC - Verifier	50	Unbefugter Zugriff auf Gesundheitsdaten im Zusammenhang mit der Prüfung von Impf-, Test-, Genesenenzertifikaten	Bei Vorlage von Impf-, Test- und Genesenenzertifikaten zur Prüfung nach [Release 2.4] könnten sowohl der Prüfer als auch umstehende Personen unbefugt Kenntnis vom Impf- oder Teststatus des CWA-Nutzers erlangen bzw. über frühere Erkrankungen, durch Anzeige der Zertifikatsart zusammen mit dem QR-Code. Daraus könnten Diskriminierungen folgen.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, TR, IV, ZB	Sollte der CWA-Nutzer entscheiden, Impf- oder Testzertifikate zur Prüfung vorzulegen, hat die prüfende Stelle Vorkehrungen zu treffen, um den CWA-Nutzern die vertrauliche Nutzung zu ermöglichen (Sichtschutzmaßnahmen, Mindestabstand zu anderen Personen u.a.). Der Prüfer kann mittels der Verifier-App erkennen, ob es sich um ein Test- oder Impfzertifikat handelt. Die Nutzung der CWA als Wallet App ist freiwillig. Mit [Release 2.5] und der Einführung einer weiteren Zertifikatsart (Genesenenzertifikat) wird dem CWA-Nutzer die Auswahl einer datensparsamen Variante der Darstellung des isolierten QR-Codes ermöglicht.			akzeptabel mit Evaluation
R4- Testcenter	51	Manipulation von QR-Code Anzeige (Attributen von Testergebnissen) und Kollision von CWA Test ID infolge einer zu niedrigen Entropie von kryptographischen Funktionen	Um die Integrität der am PoC erfassten Person und ihrer Daten zu überprüfen, wird eine Hash Funktion angewandt und deren Ergebnis in den QR-Code einkodiert. Der Hash wird aus einer bestimmten Zeichenkette kalkuliert. Hier werden 2 Parameter von der PoC erzeugt, nämlich „testid" und „salt". Der Salt wird mithilfe vorhandener Krypto-Bibliotheken kryptographisch generiert. Für die TestID werden UUIDv4 empfohlen. Selbst in Situationen wo der „Salt-" Wert immer gleich ist (z.B. wenn kryptographische Funktionen immer mit dem gleichen „Seed-" Wert initialisiert werden), verbleibt die Komplexität des Angriffes sehr hoch und zeitaufwendig. Grund hierfür sind die TestID und der Zeitstempel (der auch für die Gültigkeit des Tests sorgt) sowie die Eigenschaften der SHA-256 Hash Funktionen.	Ja	1	1	1	3	3	1	3	1	1	3	3	IG, VF, ZB	Dadurch, dass der Zeitstempel und die interne Test-ID immer anders sein werden (selbst bei eine Salt von NULL), wird genug Entropie vorhanden sein, um Kollisionen zu vermeiden. Replay-Attacke werden durch die Gültigkeitsdauer der Tests erschwert. Siehe Designentscheidung c.) B-2-1.			akzeptabel
R4 - Softwareentwickler / SAP	52	[Release 15] Verwendung von Kryptografie-Schlüsseln mit niedriger Entropie	Sofern der Kryptografie-Schlüssel, der zum Signieren der Allow-List verwendet wird, zu klein ist oder eine zu geringe Entropie aufweist, könnte ein Angreifer diesen vorhersagen/ erraten oder durch einen Brute-Force Angriff ermitteln. Ein Angreifer wäre dann in der Lage, eine eigene signierte Allow-List anzulegen bzw. die ursprüngliche Allow-List zu manipulieren.	Ja	1	1	1	3	3	1	3	1	1	3	3	IG, VF, ZB	Sicherstellung eines angemesen Entropie-Niveaus.			
R10 - Validation Service Provider/ Leistungsanbieter	53	[Release 2.15] Manipulation von Informationen zum Leistungsanbieter	Zu Zwecken der kurzfristigen Veröffentlichung Inhalt ausgeblendet. Änderungen bleiben vorbehalten.	Ja	1	0	1	3	0	3	0	1	1	1	3	IG, AT	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel

Datenschutzfolgenabschätzung (DSFA)
VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)

				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R2- Hacker	54	[Release 2.15] Manipulation des Leistungsanbieters	Zu Zwecken der kurzfristigen Veröffentlichung Inhalt ausgeblendet. Änderungen bleiben vorbehalten.	Ja	3	0	1	3	0	3	0	1	1	3	9	IG, AT, ZB	Keine Mitigationsmaßnahme in der CWA.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel mit Evaluation
R10 - Validation Service Provider/ Leistungsanbieter	55	[Release 2.15] Manipulation des "Public Keys" aufgrund interner Fehler/ Angreifer	Zu Zwecken der kurzfristigen Veröffentlichung Inhalt ausgeblendet. Änderungen bleiben vorbehalten.	Ja	1	0	0	0	4	0	4	1	1	1	4	VF, BT	Keine Mitigationsmaßnahme in der CWA.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel
R10 - Validation Service Provider/ Leistungsanbieter	56	[Release 2.15] Manipulation des Stornierungsprozesses aufgrund einer unvollständigen/ falschen Fehlerbehandlung	Zu Zwecken der kurzfristigen Veröffentlichung Inhalt ausgeblendet. Änderungen bleiben vorbehalten.	Ja	1	0	0	2	0	0	0	1	1	1	2	IG	Keine Mitigationsmaßnahme in der CWA.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel
R2- Hacker	57	[Release 2.15] Manipulation des Stornierungsprozesses aufgrund des QR-Code-Scans durch unberechtigte Dritte	Ein Angreifer könnte den QR-Code abfangen und den Validierungsprozess anstelle des CWA-Nutzers stornieren.	Ja	2	0	2	0	0	0	0	1	1	1	4	IG	Verhinderung in der Verantwortung des CWA -Nutzers. Keine Mitigationsmaßnahmen in der CWA.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel
R2- Hacker	58	Zugang/ Zugriff auf (Gesundheits-) Daten auf CWA-Komponenten (z.B. infolge der Nutzung einfacher Passwörter, fehlender IT-Sicherheit)		Ja	2	1	2	2	2	0	0	0	0	3	6	ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen a. D-11-1. Verschlüsselung der Daten beim Transport und in Storage, Sicherheitsprozesse im CWA-Bankend. Verantwortlichkeit für PoC-Backend bei PoC.			akzeptabel mit Evaluation
R4- Betreiber Server (T)	59	Unberechtigter Administratorenzugriff auf Daten auf CWA-Server		Ja	1	0	4	1	1	1	1	4	4	4	4	VT, IV, TR, ZB	AV-Verträge mit DL inkl. TOM (Berechtigungskonzept, Zugriffskontrolle, Protokollierung) und Designentscheidung a. D-11-1.			akzeptabel
R4- Betreiber Server (T)	60	Unberechtigter Administratorenzugriff auf Daten auf Poc-Server der Testcentren und Korrelation mit Daten auf CWA-Servern		Ja	1	0	4	1	1	1	1	4	4	4	4	VT, IV, TR, ZB	Verantwortung der PoC, Verträge, Leistungsbeschreibung und zusätzliche Bedingungen zur Gewährleistung von Datenschutz und Datensicherheit werden abgeschlossen.			akzeptabel
R4- Betreiber Server (T)	61	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts- und Zugriffskontrolle(TOM) für die CWA-Komponenten und die Mitarbeiter des Betreibers.		Ja	1	4	4	4	4	4	4	4	4	4	4	VT, IG, VF, A, R, IV, TR, ZB, DM	AV-Verträge mit DL inkl. TOM (Berechtigungskonzept, Zugriffskontrolle, Protokollierung).			akzeptabel
R4- Testcenter	62	Fehlende/ unzureichende Regelung/ Einhaltung von Standards zur Zugangs-, Zutritts- und Zugriffskontrolle inkl. Wiederherstellungsprozesse für Zugangsdaten (TOM) für die PoC-Komponenten/ PoC-Mitarbeiter	Mitarbeiter mit einem gültigen Konto und Multi-Faktor Authentisierung könnten Tests verwalten und durchführen, etwa auch remote, ohne ausreichende Beschränkung z.B. auf Netzwerkebene und Kontrolle durch Verantwortliche im Testzentrum vor Ort.	Ja	1	1	3	3	1	1	1	1	1	3	3	VT, IG, ZB	TOMs, Monitoring Tools, Begrenzungen zur Benutzung von zwingend 2-Faktoren (Empfehlung an die PoC; einer örtlich beschränkt), Logs der Aktivitäten der PoC-Mitarbeiter dem Admin zur Verfügung stellen. Die PoCs werden einzeln mit Mutual TLS angebunden (Zertifikate werden über einen privates CA verwaltet) und Mitarbeiter benötigen ein gültiges Konto und Multi-Faktor Authentisierung, um Tests zu verwalten und durchzuführen. Prozesse zur Wiederherstellung sind zu etablieren.	Prozesse zur Wiederherstellung sind zu etablieren.		akzeptabel mit Evaluation
R6 - Krimineller	63	Unbefugter Zugang zu/ Missbrauch der Nutzungsdaten/ Schnelltest-Profil durch "Malicious Schnelltest-Station"	Mit der CWA [Release 2.2] wird die Nutzung eines sog. Schnelltest-Profils ermöglicht. Zweck ist es, die Registrierung bei einer Schnelltest-Stelle zu vereinfachen und zu beschleunigen, sofern diese über die entsprechenden Mittel (z.B. QR-Code Scanner) verfügt. Die Daten aus dem Schnelltest-Profil sind möglicherweise für bestimmte Personen/ Personengruppen von hohem Interesse. So könnte es z.B. passieren, dass über eine „malicious" Schnelltest-Stelle für kurze Zeit Schnelltest kostenlos für CWA-Nutzer angeboten werden, um die Schnelltest-Profil-Daten von CWA-Nutzern einzuscannen und zweckwidrig/ missbräuchlich zu verwenden oder an Dritte zu verkaufen.	Ja	3	3	3	1	1	1	1	3	3	3	9	DM, VT, Z, IV, T, ZB	Anbindung von PoC erfordert Vertragsabschluss.			akzeptabel mit Evaltuation
R1-CWA-Nutzer	64	Verbreitung von Impfzertifikaten/ Testzertifikaten/ Genesenenzertifikaten über Social Media	Sofern ein CWA-Nutzer nicht sorgsam mit den Daten zu seinem Impf-, Test- oder Genesenennachweis umgeht, besteht die Gefahr, dass der QR-Code des Impf- ,Test- oder Genesenennachweises (in der CWA-App) auf Social Media oder anderweitig durch den CWA-Nutzer oder eine andere Person publiziert wird (unabsichtlich/ absichtlich). Sollte ein CWA-Nutzer seinem Impf-, Test-, Genesenennachweis mit anderen Personen teilen, können diese den QR-Code z.B. in ihrer eigenen CWA App einscannen und so an die persönlichen Informationen des CWA-Nutzers gelangen. Dies kann für den Betroffenen CWA-Nutzer durchaus auch negative Konsequenzen haben.	Ja	3	3	3	2	1	1	1	1	1	1	9	DM, VT	Aufklärung, dass nur Wallet-Funktion verwendet werden soll. Missbrauch nur dann möglich, wenn Dritter seiner Prüfpflicht nicht nachkommt und der Nachweis zweckwidrig verwendet wird. Designentscheidungen c) D-2-4.			akzeptabel mit Evalution
R1-CWA-Nutzer	65	Offenlegung der Gesundheitsdaten des CWA-Nutzers gegenüber Dritten	Sofern der Hinweis auf dem Sperrbildschirm erscheint, dass Zertifikate ablaufen, ist für Dritte einsehbar, dass ein CWA-Nutzer Corona-Zertifikate in der CWA App verwaltet. Dies würde die Information offenlegen, dass der CWA-Nutzer entweder geimpft, genesen oder getestet ist.	Ja	1	2	1	1	1	1	1	1	1	1	2	VT	Benachrichtigungen im jeweiligen Betriebssystem des Smartphones ausschalten.			
R1-CWA-Nutzer	66	[Release 2.10] Unsachgemäße Nutzung der Export-/ Druckfunktion	Mit [Release 2.10] der CWA-App ist es dem CWA-Nutzer möglich, seine in Deutschland ausgestellten DCC Zertifikate im PDF-Format zu exportieren. Sofern der CWA-Nutzer diese Funktion nutzt, entscheidet der CWA-Nutzer eigenständig, was mit dem erzeugten PDF passieren soll. Der CWA-Nutzer könnte sich z.B. dafür entscheiden, das PDF auszudrucken, um eine physische Kopie des elektronischen Zertifikats ablegen zu können. Er könnte das Zertifikat in einer unsicheren Cloud ablegen, veröffentlichen oder auch im Rahmen der Verwaltung von Zertifikaten Dritter mißbrauchen. Sollte der CWA-Nutzer die PDF-Datei (mit dem DCC Zertifikat) von seinem Smartphone über einen Netzwerkdrucker ausdrucken, könnte der Drucker den Inhalt der PDF-Datei in seinen lokalen Speicher ablegen. Eine andere Person könnte die im Drucker abgespeicherte Datei dann – ohne Wissen des Nutzers - erneut ausdrucken. Wenn der CWA-Nutzer einen frei zugänglichen Netzwerkdrucker auswählt, könnte es passieren, dass Unbefugte den Ausdruck entwenden und missbräuchlich verwenden.	Ja	3	1	3	1	1	1	1	2	1	3	9	VT, ZB	Der CWA-Nutzer wird in der CWA App darauf hingewiesen, sorgfältig mit der Exportfunktion umzugehen; die Zertifikate nicht zu veröffentlichen o.ä.			akzeptabel mit Evaluation
R2- Hacker	67	[Release 2.10] Auslesen der PDF-Datei-Inhalte im Netzverkehr des ausgewählten Druckers	Sofern der CWA-Nutzer sein DCC Zertifikat exportiert und über eine unsichere Verbindung z.B. einen ungeschützten Drucker übermittelt, könnte es einem Angreifer gelingen, die Kommunikation zu bemerken und abzuhören. Wenn der Angreifer diese Netzwerkpakete speichern/einsehen kann, dann könnte er vermutlich auch das übermittelte DCC Zertifikat aus dem Datenverkehr extrahieren.	Ja	2	1	3	1	1	1	1	1	1	1	6	VT	Allgemeine Sorgfalt bei Auswahl des Druckers für sensible personenbezogene Daten.			akzeptabel
	68	**5) Verweigerung der Betroffenenrechte (Betrachtung der Unterstützung durch SAP/T)**																		
R4 - Softwareentwickler / SAP	69	Fehlende Verfügbarkeit des Testzertifikates nach Verlust	Berechtigte könnten ein auf ihrer CWA-App nicht mehr verfügbares Testzertifikat innerhalb des Gültigkeitszeitraums nicht erneut abrufen. Damit könnten ggf. Rechte und Freiheiten nicht mehr ausgeübt werden.	Ja	2	1	1	1	3	1	3	1	1	1	6	VT, BL	Aktuell kann das Testzertifikat durch die CWA-App nur einmal abgerufen werden. Diese haben nur eine begrenzte Gültigkeit, des weiteren bestehen Alternativen für Betroffene (eigener Ausdruck / CovPass-App).	Eine entsprechende Funktion ist für ein kommendes Release [Release 2.10] geplant und wird gerade geprüft (Backup-Funktion, Download-Button).		akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	70	Fehlende Umsetzung der Widerrufsmöglichkeit, speziell für Schnelltest-Anbindung und Anzeige		Ja	3	2	2	2	1	1	1	2	2	2	6	IV, T, ZB	Widerruf der Einwilligung per Einstellung möglich (Designentscheidung aD-2-2c), auf dem Servern keine Herstellung des Personenbezugs zur Erfüllung Betroffenenrechte (Designentscheidung a D-8-1).			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	71	Nichtbeachtung von Auskunftsrechten (keine Verpflichtung zur Herstellung Personenbezug) - Art. 11		Ja	1	4	0	0	0	0	0	0	4	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte (Designentscheidungen a D-8-1).			akzeptabel

Datenschutzfolgenabschätzung (DSFA)
VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)

				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R4 - Softwareentwickler / SAP	72	Nichtbeachtung von Löschungsersuchen, Berichtigungsersuchen - Art. 11		Ja	1	0	0	1	0	4	0	4	0	0	4	DM	Designentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte (Designentscheidungen a. D-8-1).			akzeptabel
R4 - Softwareentwickler / SAP	73	Fehlende Übertragbarkeit		Ja	1	0	0	0	0	0	0	4	0	4	4	IV	Designentscheidung/ Pseudonymisierung, keine Herstellung Personenbezug zur Erfüllung Betroffenenrechte (Designentscheidungen a. D-8-1).			akzeptabel
R4- Betreiber Server (T)	74	Fehlende/ unzureichende Löschung der Daten auf den CWA-Servern bei Löschersuchen		Ja	3	3	3	0	0	0	0	3	3	3	9	DM, VT, IV, TR, ZB	Siehe Designentscheidung a. D-2-2c, Restrisiken ausgewiesen in DSK-Rahmenkonzept v1.13 Kap. 14.28.20 - 14.28.23.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	75	Fehlende/ unzureichende Löschung der Daten bei "In-App-Reset" (nur Android)	Im Falle eines „In-App Resets" werden möglicherweise nicht alle persönlichen Daten, die im Rahmen der App-Nutzung vom Android Betriebssystem erstellt werden, vollständig gelöscht. Ein Angreifer könnte hierauf unberechtigt Zugriff erhalten, wenn er in der Lage wäre, das Android-Gerät zu rooten.	Ja	2	3	3								6		Um eine vollständige Löschung aller Daten der CWA (und der von Android Betriebssystem erstellen Logs) sicherzustellen, kann/ muss die App de-installiert werden (Beschreibung in DSK CWA App v2.2, Kap. 7.4.17).			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	76	Fehlende/ unzureichende Löschung der Daten bei De-Installation der App/ Zurücksetzen der App (Frontend)		Ja	1	4	0	0	0	0	0	4	0	4	4	DM	Siehe Ausführungen zur Löschung in dem DSK CWA und die Optimierung des End-of-Live Verhaltens der App (Designentscheidung a. D-9-9).			akzeptabel
R8- Behörden	77	Fehlende Invalidierung-/ Revoke-Funktion für Schnelltestergebnisse	Auch wenn sich die Zuverlässigkeit von Schnelltests verbessert hat, so kann dennoch nicht ausgeschlossen werden, dass ein „positives" Corona-Schnelltest Ergebnis einer Überprüfung mittels PCR Test nicht standhält (False-Positive Meldung). In einem solchen Fall müsste das Schnelltestergebnis zurückgezogen werden können, um mögliche Nachteile für den CWA-Nutzer ausschließen zu können. Wenn Warnungen erfolgten, die auf einem False-Positive-Schnelltest basierten, entstehen auch durch die Gewarnten Nachteile, die sich ggf. freiwillig in Quarantäne begaben.	Ja	2	2	2	2	0	0	0	3	0	3	6	IV, ZB	Trennung von PCR-/ Schnelltestergebnisanzeigen inkl. der jeweiligen Berücksichtigung der Chronologie der Testzeitpunkte, um „alte" Testergebnisse durch „neuere " überschreiben zu können und so eine korrekte und konsistente Anzeige zu ermöglichen.		Implementierung einer "Rückruf-Möglichkeit" für Warnungen	akzeptabel mit Evaluation
R1-CWA-Nutzer	78	[Release 2.5] Verweigerung der Betroffenenrechte bei Nutzung der Familienfunktion	Mit [Release 2.5] wird dem CWA-Nutzer die Möglichkeit eröffnet, DCC-Zertifikate anderer Personen in seiner CWA-App zu speichern. Eine Löschung erfolgt nicht automatisch, sondern muss manuell vom CWA-Nutzer initiiert werden. Für Familienmitglieder, deren Zertifikat verwaltet wird, besteht das Risiko, dass die Zertifikate nicht gelöscht werden, selbst wenn dies von diesem gewünscht wird. Es sind auch Fälle denkbar, in denen CWA-Nutzer die Funktion nicht nur für Familienangehörige nutzen, sondern darüber hinaus, etwa im Rahmen einer Reise oder Klassenfahrt.	Ja	2	2	2	1	1	1	1	2	2	2	4	DM, VT, TR, IV, ZB	Siehe Risikomatrix VT_1_2_4, Zeile 104 (Verweigerung von Betroffenenrechten durch CWA-Nutzer im Rahmen KTB), keine automatische Löschung (siehe Designentscheidung D-9-5e) oder andere technische Mitigationsmaßnahmen.			akzeptabel
R8- Behörden	79	Nichtgewährung von Betroffenenrechten im Zusammenhang mit dem Widerruf gültiger Zertifikate.	Der Widerruf in der CWA erfolgt aufgrund eines Identifiers (z.B. Aussteller/ID). Betroffene können damit CWA-Nutzer sein, denen rechtmäßig gültige Zertifikate ausgestellt wurden. Werden diese automatisch widerrufen, müssen insbesondere Auskunfts- und Berichtigungsansprüche gewährt werden.	Ja	3	2	1	1	2	1	1	2	2	2	6	DM, TR, ZB	Die CWA-Nutzer werden auf verschiedenem Wege infomiert und auf die ausgebenden Stellen verwiesen. Wird ein zulässiges Zertifikat widerrufen, werden niedrigschwellige Möglichkeiten geschaffen, das Zertifikat zu erneuern.			akzeptabel mit Evaluation
R8- Behörden	80	[Release 2.15] Nichtgewährung Widerrufsrecht bei der Überprüfung von Zertifikaten über den Validierungsservice	Nachdem der CWA-Nutzer sein Einverständnis zur Verarbeitung der Daten gegeben hat, ist es ihm nicht möglich, dieses über einen einfachen Weg wieder zu widerrufen.	Ja	2	0	3	0	0	0	0	3	0	3	6	VT, IV, ZB	Für die CWA-App muss keine Widerrufsmöglichkeit vorgesehen werden, da die App keine Daten speichert, die von einem Widerruf betroffen wären und für die Realisierung der Widerrufsfunktion weitere pD erforderlich wären.			akzeptabel mit Evaluation
	81	**6) Verwendung der Daten zu inkompatiblen Zwecken**																		
R8- Behörden	82	De-Anonymisierung/ De-Pseudonymisierung von Nutzern anhand von optionalen Lokalisierungsdaten		Ja	3	3	3	3	0	0	0	3	3	3	9	ZB, TR, IV, VT, IG, DM	Empfehlung des RKI zur Einhaltung Datenschutz und Datensicherheit (keine Aufhebung der Pseudonymisierung).			akzeptabel mit Evaluation
R1-CWA-Nutzer	83	[Release 2.1] Nutzung der negativen Schnelltestergebnisse für Verifikation oder als "Eintrittskarte"	Die Integration der Schnelltestergebnisaufruf in der App mit [Release 2.1] dient nicht der Verifikation oder dem Ausweisen der Nutzer als negativ oder positiv getestet. Die Funktion als "Eintrittskarte" könnte trotzdem (ohne Rechtsgrundlage) von Dritten angefragt werden. Aktuell ist es nicht möglich, den angezeigten Schnelltest zu verifizieren. Ein Dritter könnte nur die Anzeige auf dem Smartphone des CWA-Nutzers sehen. Zwar zeigt die eingebaute und im Sekundentakt zurückzählende Uhr an, dass nicht nur ein Bild vorgezeigt wird, aber die Fälschung von Negativanzeigen ist auch relativ einfach möglich, so dass die Integrität verletzt wird.	Ja	3	4	4	0	0	0	0	1	1	4	12	VT, IG, ZB	Information der CWA-Nutzer, dass die Funktionalität nur für den privaten Gebrauch gedacht ist und keine Verpflichtung zum Vorzeigen an Dritte besteht (Designentscheidungen c D-3.2-2).		Verhältnismäßigkeit Restrisiko ist generell bewertet (siehe DSFA-Bericht), Vertrauen auf angemessenes Verhalten durch Dritte	bedingt akzeptabel
R4- Testcenter	84	Zweckwidrige Speicherung oder (Weiter-)Nutzung des Schnelltest-Profils in den PoC	Durch die Nutzung/Unterstützung vom PoC bekommt dieser auf dem Markt eine bevorzugte Stelle. Diese Stelle ermöglicht es dem Anbieter, in einem großen Umfang personenbezogene Daten zu erfassen und zu verarbeiten. Es kann daher nicht ausgeschlossen werden, dass die von der CWA-App über den CWA-Nutzer bereitgestellten Daten nicht auch für andere Zwecke weiterverwendet werden, etwa auch per Exportfunktion eine Übermittlung an Gesundheitsamt oder Dritte.	Ja	1	3	4	1	1	1	1	3	3	3	4	DM, VT, IV, T, ZB	Verträge mit PoC bestimmen den Umfang der DV im Zusammenhang mit der CWA. PoC erheben die Daten aufgrund eigener Rechtsgrundlage, wenn Schnelltest-Profil nicht genutzt wird.			akzeptabel
R1-CWA-Nutzer	85	Teilung Schnelltest-Profil/ Fake-Schnelltest-Profil über Social Media	Ein CWA-Nutzer könnte ein Foto mit dem Schnelltest-Profil oder das Schnelltest-Profil selbst auf Social Media stellen. Dieses könnte dann von Dritten ausgewertet bzw. verkauft werden. Risikobewertung [Release 2.6]: Sofern ein Schelltestprofil geändert wird, so werden die neuen Daten genutzt, um im Rahmen der Anmeldung zu einem Schnelltest diese Daten für den neuen Schnelltest weiter nutzen zu können. Dies führt dazu, dass möglicherweise Schnelltests mit unterschiedlichen/ abweichenden Meta-Daten auf dem Smartphone des Nutzers abgelegt werden. Die neu eingegebenen Daten können zudem von Metadaten, die für PCR Tests-/ Zertifikate genutzt werden, abweichen. Dies könnte bei der Anzeige (inkl. gewisser Mata-Daten) zu Verunsicherungen beim Nutzer führen. Auch könnten sich Personen verwirrt zeigen, sofern die Daten/ Zertifikate/ Testergebnisse überprüft werden.	Ja	2	2	4	1	1	1	1	2	2	2	8	VT	Keine technischen Mitigationsmaßnahmen möglich; Verantwortung der CWA-Nutzer, Aufklärung und öffentliche Informationskampagnen des BMG			akzeptabel mit Evaluation
R1-CWA-Nutzer	86	Teilung negatives Testergebnis über Social Media	Ein CWA-Nutzer könnte ein Foto mit dem negativen Testergebnis oder das Testergebnis selbst auf Social Media stellen. Dieses könnte dann von Dritten ausgewertet bzw. verkauft werden.	Ja	2	2	4	1	1	1	1	2	2	2	8	VT	Auf der Anzeige von Android-Geräten wird ein "Counter" angezeigt, womit ein Testnachweis durch Screen-Shot erschwert wird. Darüber hinaus sind keine technischen Mitigationsmaßnahmen möglich; Verantwortung der CWA-Nutzer. Aufklärung und öffentliche Informationskampagnen des BMG			akzeptabel mit Evaluation
R5-Arbeitgeber, Versicherungen	87	CWA wird als Nachweis-App für Impf-/ Test- und Genesenenzertifikate angesehen, nicht als Wallet App	Fügt der CWA-Nutzer seine Impfnachweise, Testzertifikate und/ oder Genesenenzertifikate in die CWA-App hinzu, ermöglicht diese es dem CWA-Nutzer, die jeweiligen Nachweise anzuzeigen (QR-Code + Details auf dem entsprechenden Screen). 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. Wird daher auf die Überprüfung verzichtet, kann dies zu falschen Schlüssen über den Impfstatus der Person führen. Entsprechendes gilt für die Testzertifikate und Genesenenzertifikate in der CWA.	Ja	3	1	1	3	1	1	1	1	1	3	9	VT, ZB	Aufklärung, dass nur Wallet-Funktion; Missbrauch nur dann möglich, wenn Dritter seiner Prüfpflicht nicht nachkommt und zweckwidrig als Nachweis verwenden lässt (Designentscheidungen c) D-2-4 und D-2-5).			akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R1-CWA-Nutzer	88	[Release 2.6] DCC-Business-Rules: CWA wird als "Prüf-App" für Zertifikate angesehen, hinsichtlich lokaler/ mitgliedstaatlicher Regelwerke	Risikobetrachtung [Release 2.6]: In Deutschland gibt es offiziell geprüfte und für diesen Zweck freigegeben Prüf-Apps (z.B. die Cov-Pass App). In der CWA ist das Feature zur Validierung der Zertifikate lediglich als „Komfortfunktion für den Nutzer" vorgesehen. Sofern es zu Unterschieden in der Anzeige der Verifikationsergebnisse in der CWA-App im Vergleich zu der lokalen Validierungs-App kommen sollte, könnte dies zu Nachteilen für den CWA-Nutzer führen, der sich auf die Richtigkeit der Komfortfunktion verlassen hat. Sofern die Regelwerke nicht konsistent sind und die Konsistenz nicht über den gesamten Lebenszyklus sichergestellt werden kann (Erstellung – Verteilung – Nutzung), könnten falsche/ manipulierte Regeln zur Validierung in der CWA-App herangezogen werden. Das könnte sowohl zu eine Reputationsschaden für die CWA-Lösung als auch zu individuellen Problemen für die CWA-Nutzer führen.	Ja	3	1	1	3	1	1	1	1	3	3	9	IG, TR, ZB	Der Nutzer wird in der CWA-App darüber informiert, dass die Validationsregeln seitens der EU Länder aktualisiert werden können und dass das Fehlen von Regeln nicht den Schluss erlaubt, dass ein DCC Gültigkeit hat. Verwaltung des Lebenszyklus der DSC (Signierende Zertifikate). Automatische Regelwerk- und DCC-Überprüfung bei Regelwerkaktualisierungen.			akzeptabel mit Evaluation
R2- Hacker	89	DCC-Business-Rules: CWA wird als "Prüf-App" für Zertifikate angesehen, hinsichtlich fehlender, fehlerhafter, veralteter, bewusst oder unbewusst manipulierter lokaler/ mitgliedstaatlicher Regelwerke (fehlerhafte Auswertung EU Zertifikatsprüfung mittels CWA)	Sofern ein Land keine Regelwerke zur Zertifikatsprüfung bereitstellt, muss sichergestellt werden, dass der Nutzer transparent darüber informiert wird. Sofern das nicht erfolgt, könnte der CWA-Nutzer vermuten, dass eine Ein-/Ausreise ohne Einschränkungen möglich ist. Sofern das nicht der Fall ist, könnte das sehr negative Auswirkungen auf den CWA-Nutzer haben (Beschränkung Reisefreiheit, Diskriminierung). Sofern ein CWA-Nutzer in seiner CWA-App „fälschlicherweise" angezeigt bekommt, dass seine Zertifikate gültig sind, kann das extrem negative Konsequenzen für den Nutzer haben, wenn er z.B. Reisen möchte und die lokalen Regelwerke eine Einreise nicht zulassen.	Ja	1	1	1	3	1	1	1	1	3	3	3	IG, TR, ZB	Der Nutzer wird in der CWA-App darüber informiert, dass die Validationsregeln seitens der EU Länder aktualisiert werden können und dass das Fehlen von Regeln nicht den Schluss erlaubt, dass ein DCC Gültigkeit hat. Verwaltung des Lebenszyklus der DSC (Signierende Zertifikate). Automatische Regelwerk- und DCC-Überprüfung bei Regelwerkaktualisierungen.	Einsatz von digitalen Signaturen und ggf. Versionierung für DSC-Listen und Regelwerke.		akzeptabel mit Evaluation
R2- Hacker	90	Missbrauch/ Sammlung von pD mittels Anzeige von Impf-, Test-, Genesenenzertifikaten in der CWA-App	Sollte ein CWA-Nutzer seinen Impfnachweis in der CWA-App einem Dritten vorzeigen, um nachzuweisen, dass er geimpft wurde bzw. sein Testzertifikat, dass er getestet wurde, könnte diese Person Informationen (wie z.B. das Impfdatum oder den Impfstoff oder den Teststatus) über den CWA-Nutzer erhalten. Auf Grund der in Deutschland vorgebenden Impf-Priorisierung gemäß der Impfgruppen ist es unter Umständen möglich, Rückschlüsse auf die Gruppenzugehörigkeit und/oder die Berufszugehörigkeit des CWA-Nutzers zu ziehen. Auch sind Diskriminierungen denkbar, durch z.B. den Rückschluss vom Testergebnis auf fehlende Impfbereitschaft o.ä.	Ja	3	3	3	1	1	1	1	1	1	3	9	DM, VT, ZB	Funktion ist freiwillig. Aufklärung, dass nur Wallet-Funktion (Designentscheidungen c) D-2-4 und D-2-5).			akzeptabel mit Evaluation
R6 - Krimineller	91	Malicious Verifier App	Zur Überprüfung, ob es sich um ein gültiges Testzertifikat handelt, kommt eine spezielle App zum Einsatz, die die Echtheit des Zertifikat überprüfen kann. Diese App kann zur Validierung des Testzertifikates genutzt werden. Es ist daher vorstellbar, dass ein Angreifer sich selber eine Validierungs-App baut und alle eingescannten QR-Code als valide markiert. Dadurch wäre es möglich, beliebigen Personen auch ohne valides Testzertifikat Zugang zu einem Ort oder Veranstaltung zu gewähren. Zudem wäre es auch möglich, die modifizierte Validierungs-App dazu zu nutzen, um die Daten aus den QR-Code auszulesen und für anderen Zwecke zu missbrauchen.	Ja	3	3	3	3	1	3	1	3	3	3	9	DM, VT, IG, IV, TR, ZB	Sensibilsierung der CWA-Nutzer. Keine Mitigation im Rahmen der CWA möglich (Verifier out of scope).			akzeptabel mit Evaluation
R1-CWA-Nutzer	92	[Release 2.5] Zweckwidrige Verwendung von Daten Dritter im Rahmen der Funktion Familienzertifikate	Mit [Release 2.5] wird dem CWA-Nutzer die Möglichkeit eröffnet, DCC-Zertifikate anderer Personen in seiner CWA-App zu speichern. Zweck ist es, dem CWA-Nutzer hiermit das Halten von Zertifikaten von Familienmitgliedern zu ermöglichen, um die damit zusammenhängenden Rechte und Freiheiten für die gesamte Familie ermöglichen zu können. Die Funktion könnte für andere Zwecke missbraucht werden, etwa durch Reiseleiter, die die Zertifikate von Reisenden einscannen und dann Impfregister o.ä. erstellen.	Ja	2	3	2	1	1	1	1	3	2	3	6	DM, IV, ZB	Hinweis an CWA-Nutzer erfolgt, dass dies eine Funktion für Familienzertifikate ist.	In [Release 2.15] oder einen Hot-Fix Release zum [Release 2.15] geplant (Update vom 10.12.2021): Begrenzung der Anzahl der Personen für die Qr Codes (DCC's) eingelesen werden können auch maximal 20 Personen. Wenn DCC's für mehr als 10 Personen eingelesen werden, dann erhält der Nutzer der einlesenden CWA einen Hinweis auf die begrenzte Personenzahl, sobald er ein DCC einen zusätzlichen Person einliest. Diese Prüfung erfolgt lokal auf dem Smartphone des Nutzers. Sobald DCC's von 20 Personen eingelesen wurden, können keine DCC's von zusätzlichen Personen eingelesen werden. Weitere Maßnahmen sind in Prüfung.		akzeptabel mit Evaluation
R2- Hacker	93	[Release 2.15] Erschleichen von Berechtigungen und Nutzung für eigene Zwecke	Zu Zwecken der kurzfristigen Veröffentlichung Inhalt ausgeblendet. Änderungen bleiben vorbehalten.	Ja	1	0	0	3	0	0	0	1	1	3	3	IG, ZB	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel
R2- Hacker	94	[Release 2.15] Erschleichen von Berechtigungen und Nutzung für eigene Zwecke	Zu Zwecken der kurzfristigen Veröffentlichung Inhalt ausgeblendet. Änderungen bleiben vorbehalten.	Ja	3	0	0	3	0	0	0	1	1	3	9	IG, ZB	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.	Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		akzeptabel mit Evaluation
	95	**7) Verarbeitung nicht richtiger Daten**																		
R4- Testcenter	96	Falsche Aufnahme des Namens	Durch die Vielfalt von Kulturen/ Sprachen ist es möglich, dass der Namen falsch aufgenommen wird, eine falsche Zuordnung erfolgt und die Schnelltestanzeige nicht mit dem richtigen Namen des CWA-Nutzers erscheint.	Ja	1	1	1	2	1	1	1	1	1	2	2	IG, ZB	Sensibilisierung der Mitarbeiter, Verifikation mit einem offiziellen Personaldokument durchzuführen.			akzeptabel
R4- Testcenter	97	Unbewusste/ fahrlässige falsche Zuordnung eines "negativen Schnelltestergebnisses" zu einer mit Corona infizierten Person oder falsche Zuordnung eines "positiven Schnelltestergebnisses" zu einer nicht-infizierten Person (Vertauschte Test-ID) durch PoC	Sofern die IDs, die zur Zuordnung von Tests zu getesteten Personen im Testcenter genutzt werden, vertauscht oder falsch zugeordnet werden, kann es passieren, dass einer an Corona infizierten Person fälschlicherweise ein "negatives Schnelltestergebnis" an die CWA-App übermittelt und dort angezeigt wird. Sofern die GUID's/Proben IDs zur Zuordnung von Tests zu getesteten Personen vertauscht oder falsch zugeordnet werden sollten, kann nicht ausgeschlossen werden, dass Testergebnisse an die „falschen" Personen übermittelt werden. Sofern die Testergebnisse „namentlich" übermittelt werden, würde das Schnelltestergebnis, der Name, das Geburtsdatum, … einer konkreten Person einer anderen Person dargestellt und verfügbar gemacht werden.	Ja	1	1	3	3	1	1	1	1	1	2	3	VT, IG, ZB	Schulung des Personals, Festlegung strikter/ überprüfbarer Validierungsprozesse, Planung geeigneter TOM's, Verwendung von ausgedruckten Probenetiketten zur Kennzeichnung der Proben.			akzeptabel
R4- Testcenter	98	Unbewusste/ fahrlässige falsche Zuordnung eines "negativen Schnelltestergebnisses" zu einer mit Corona infizierten Person oder falsche Zuordnung eines "positiven Schnelltestergebnisses" zu einer nicht-infizierten Person (Vertauschte Test-ID) durch Drittanbieter (DM, Testiabor)	Sofern die IDs, die zur Zuordnung von Tests zu getesteten Personen im Testcenter genutzt werden, vertauscht oder falsch zugeordnet werden, kann es passieren, dass einer an Corona infizierten Person fälschlicherweise ein "negatives Schnelltestergebnis" an die CWA - App übermittelt und dort angezeigt wird. Sofern die GUID's/Proben IDs zur Zuordnung von Tests zu getesteten Personen vertauscht oder falsch zugeordnet werden sollten, kann nicht ausgeschlossen werden, dass Testergebnisse an die „falschen" Personen übermittelt werden. Sofern die Testergebnisse „namentlich" übermittelt werden, würde das Schnelltestergebnis, der Name, das Geburtsdatum, … einer konkreten Person einer anderen Person dargestellt und verfügbar gemacht.	Ja	2	1	3	3	1	1	1	1	1	2	6	VT, IG, ZB	Schulung des Personals, Festlegung strikter/ überprüfbarer Validierungsprozesse, Planung geeigneter TOM's, Verwendung von ausgedruckten Probenetiketten zur Kennzeichnung der Proben.			akzeptabel mit Evaluation
R4- Testcenter	99	Bewusst falsche Zuordnung eines Testergebnisses zu einer anderen Person durch das Personal im Testzentrum	Sofern ein negatives Schnelltestergebnis für eine getestete Person zu Vergünstigungen führt, könnte diese Person andere Personen die „sicher" nicht infiziert sind, zum Test schicken und deren „negatives" Testergebnis für sich selber – z.B. inkl. Anzeige des Ergebnisses in der App – nutzen, um z.B. Zugang zu einer Einkaufsmöglichkeit zu bekommen, obwohl möglichwese eine Corona Infektion vorliegt.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Festlegung strikter/ überprüfbarer Validierungsprozesse, Planung geeigneter TOM's/ Prüfung des Ausweises der getesteten Person.		Schutz der Inhalte des Barcodes vor Manipulationen/ Digitale Signatur zur Verifikation // Eine Signatur in dem Sinne wird nicht durchgeführt. Im Falle von Personenbeziehbaren Tests (also „Eintrittskarte"), werden die Daten gehasht und der Hash als ID (nicht mehr die GUID) im Backend verwendet. Damit lässt sich verifizieren, ob ein User seinen Namen nach/ während des Tests in der App ändert oder einen anderen Test pullt.	akzeptabel mit Evaluation

Datenschutzfolgenabschätzung (DSFA) VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
R4- Testcenter	100	False Positive - Schnelltests	Auch wenn sich die Zuverlässigkeit von Schnelltests verbessert hat, so kann dennoch nicht ausgeschlossen werden, dass ein „positives" Corona-Schnelltest fälschlicherweise zustande gekommen ist (falsche Testdurchführung/…). Dadurch könnten sich Nutzer grundlos in „Selbstquarantäne" begeben.	Ja	2	1	3	3	1	1	1	1	1	3	6	VT, IG, ZB	Korrekte Beschreibung der Limitationen/ begrenzten Aussagekraft der Schnelltestergebnisse und Darlegung konkreter nächster Schritte, um zu prüfen ob es sich eine ein „falsches positives Schnelltestergebnis" handelt oder ob tatsächlich eine Corona-Infektion vorliegt. Idealerweise würden die Handlungsanweisungen „deutschlandweit" offiziell kommuniziert (gesetzlich geregelt), damit Unklarheiten vermieden werden können. Das gilt auf für die Regeln zur Aufhebung der Quarantäne (sog. "Frei-Testen").			akzeptabel mit Evaluation
R1-CWA-Nutzer	101	Verschicken bewusst falscher Warnungen an andere CWA-Nutzer	Sofern es einem Nutzer gelingen sollte, falsche „positive" Schelltestergebnisse zu erhalten (z.B. durch die Bereitstellung von Proben positiv auf Corona getesteter Personen), könnte er andere CWA-Nutzer fälschlicherweise vor mögliche Risiken warnen.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Sicherstellung entsprechender Test-Vorgehensweisen in PoC und Festlegung entsprechender TOM's, um auch technische Missbrauchsoptionen zu vermeiden.			akzeptabel mit Evaluation
R6 - Krimineller	102	Verkauf "negativer" Schnelltestergebnisse	Sofern ein negatives Schnelltestergebnis für eine getestete Person zu Vergünstigungen führt, könnte Interesse bestehen – gegen entsprechende Bezahlung – negative Testergebnisse „on-demand" anzubieten und zu verkaufen.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Festlegung strikter/ überprüfbarer Validierungsprozesse, Planung geeigneter TOM's/ Prüfung des Ausweises der getesteten Person.		Schutz der Inhalte des Barcodes vor Manipulationen/ Digitale Signatur zur Verifikation.	akzeptabel mit Evaluation
R6 - Krimineller	103	Ausnutzung der Schnelltests durch Bevölkerungsgruppen	Bestimmte Bevölkerungsgruppen könnten ein Interesse daran haben, die Schnelltests für ihre Zwecke auszunutzen. Es ist vorstellbar, dass ein Anteil dieser Bevölkerung möglicherweise Zugang zu Schnelltest-Zentren haben, wo sie sich und anderen der Bevölkerungsgruppe negativ/positive Schnelltest-Ergebnisse ausstellen könnten. Diese Ausgestellten Testergebnisse würde dann auch möglicherweise in der CWA-App landen. Sollte der Schnelltest positiv sein, könnte dieser dazu verwendet werden, um andere CWA-Nutzer damit zu warnen. Ziel eines solchen Angriffs wäre es, viele Personen ein erhöhtes Risiko in der CWA-App anzuzeigen. •Sollte der Schnelltest negativ sein, könnte die CWA App missbraucht werden, um Zugänge zu bestimmten Veranstaltungen zu erhalten.	Ja	3	1	3	3	1	1	1	1	1	2	9	VT, IG, ZB	Festlegung strikter/ überprüfbarer Validierungsprozesse, Planung geeigneter TOM's/ Prüfung des Ausweises der getesteten Person.		Schutz der Inhalte des Barcodes vor Manipulationen/ Digitale Signatur zur Verifikation.	akzeptabel mit Evaluation
R1-CWA-Nutzer	104	Ausnutzung der Fehleranfälligkeit der Schnelltests (Durchführung von mehreren Schnelltests, bis ein Test negativ ist)	Auch wenn sich die Zuverlässigkeit von Schnelltests verbessert hat, so kann dennoch nicht ausgeschlossen werden, dass ein „positives" Corona-Schnelltest Ergebnis durch falsche Anwendung des Tests oder durch Manipulationen bei der Testdurchführung zu einem falschen „negativen" Testergebnis führt (False Negative). Durch die mehrfache Testdurchführung könnte einen Nutzer versuchen, die für ihn negativen Konsequenzen eines positiven Schnelltestergebnisses zu umgehen, indem er so lange weitere Tests durchführen lässt/durchführt, bis ein Test „negativ" ausfällt.	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Technische Mitigation schwer umsetzbar, wenn es keine zentralen System zum Monitoring der individuellen Schnelltestungen der Nutzer gibt, die einen solchen Missbrauch erschweren würden.		Möglicher Einbau eines Zählers, um festzustellen ob jemand versucht, sich ein negatives Schnelltestergebnis einzuholen (False Negative) anstatt eine Verifikation durch PCR-Test.	akzeptabel mit Evaluation
R1-CWA-Nutzer	105	Manipulation von Daten: Fake-Anzeige von negativen Testergebnissen in der CWA	Nutzer oder auch Hacker könnten versuchen, die Anzeige des Schnelltestergebnisses (eines früheren negatives Tests) so zu manipulieren, dass er in der App wie ein aktuelles reales Schnelltestergebnis aussieht. Wenn diese Anzeige als "Eintrittskarte" nutzbar wäre, könnte der CWA-Nutzer damit diese unrichtigen Daten veröffentlichen, selbst Vorteile erlangen und das Vertrauen in die Richtigkeit der Funktion durch andere stören.	Ja	1	1	3	3	1	1	1	1	1	3	3	VT, IG, ZB	Um die Integrität von QR-Code und Test zu erhöhen, werden digitale Signaturen verwendet, die auch den Zeitstempel und die personenbezogenen Daten umfassen. App und Backend prüfen diese Signaturen.			akzeptabel
R1-CWA-Nutzer	106	Manipulation von Daten: Manipulation von Daten mit verzögerter QR-Code-Registrierung	Wenn kein Validierungsprozess für die angezeigten Daten umgesetzt wird, besteht die Möglichkeit, diese Daten zu manipulieren. Ohne Validierung der Daten, können auch eine Vielfalt von Angriffe niedriger technischer Komplexität umgesetzt werden. Die Auswirkungen sind durchaus höher, indem Testergebnisse auf der CWA-App als Nachweis angewendet werden können.	Ja	1	1	3	3	1	1	1	1	1	3	3	VT, IG, ZB	Zeitstempel in den gehashten und signierten Daten werden hinzugefügt und geprüft.			akzeptabel
R2- Hacker	107	Manipulation von Daten: Manipulation von Schnelltest-Nutzerdaten	Wenn Nutzerdaten nicht verifiziert werden, könnte ein gesunder Nutzer einen Test registrieren, und seine persönlichen Daten im QR Code durch jemand anderen ersetzen.	Ja	1	1	3	3	1	1	1	3	3	3	3	VT, IG, ZB, T, IV	Einsatz von Digitalen Signaturen.			akzeptabel
R4- Testcenter	108	[Release 2.4] Ausstellung und Signierung von Impfzertifikaten/ unrichtigen Testzertifikaten über PoC (Malicious PoC)	Mit [Release 2.4] werden Testzertifikate in die CWA integriert. Es droht folgendes Risiko: Ein „Malicious PoC" übergibt anstatt des Hashes eines Testzertifikates den Hash eines Impfzertifikats an den DCC Server, welches dann signiert wird. Da durch die CWA und den DCC nur Hashwerte verarbeitet werden und keine Prüfung auf Richtigkeit erfolgt, erhält ein ggf. Unberechtigter über den PoC ein vermeintlich gültiges Impfzertifikat, erschleicht sich damit weitgehende Erleichterungen und gefährdet u.U. Dritte. Dieses Risiko besteht auch, wenn der Verifier bei der Prüfung nicht erkennen kann, ob es sich um ein Impf- oder Testzertifikat handelt oder dies bewusst ignoriert.	Ja	2	1	1	4	1	1	1	4	4	4	8	IG, IV, TR, ZB	Eine Prüfung des von den Testcentern übergebenen Payloads auf Richtigkeit erfolgt durch die CWA und den DCC Server nicht, da nur Hashes übertragen werden. Die Fälschung von Zertifikaten durch PoC (Mitarbeiter) erfüllt ggf. einen Straftatbestand. Um die Risiken durch ein Malicious PoC zu minimieren, werden zunächst nur als zuverlässig ausgewählte PoC an den DCC Server angebunden.	Um in der Verifier-App den Typ des Zertifikates unterscheiden zu können, soll durch die CovPass-App das von der DCC-Verordnung der EU spezifizierte Feld „extended key usage" implementiert werden und die Funktion in der CWA erst dann zur Verfügung stehen (Designentscheidungen c.) D-2-5).		akzeptabel mit Evaluation
R1-CWA-Nutzer	109	Erschleichung von Freiheiten durch legitime/ modifizierte Impfzertifikate/ Testzertifikate/ Genesenenzertifikate anderer Personen	Es besteht die Gefahr, dass ein Angreifer sich einen Impfnachweis einer anderen (geimpften) Person besorgt und diesen in seiner CWA-App einscannt (mittels QR-Code). Die CWA-App würde den Impfnachweis erkennen und dementsprechend in der CWA-App anzeigen. Alternativ könnte der Angreifer versuchen den QR-Code zu manipulieren, bevor der QR-Code von dem Angreifer in dessen CWA-App eingescannt wird. Das würde dazu führen, sofern der Angreifer die (modifizierten) Daten richtig aufbereitet, dass die CWA-App modifizierte Daten anzeigen würde. Der Angreifer könnte sich so möglicherweise unberechtigterweise Freiheiten oder sonstige Privilegien erschleichen. Dieses Risiko wurde auch für [Release 2.4] und die Testzertifikate betrachtet. Eine Erhöhung der Risikozahl erfolgt nicht; es droht insoweit kein höherer Schaden durch das Testzertifikat. Das gleiche gilt für [Release 2.5] (Genesenenzertifikat).	Ja	3	1	3	3	1	1	1	1	1	3	9	VT, IG, ZB	Das Gewähren von Freiheiten und Privilegien muss an eine Prüfung der in der CWA-App angezeigten Impfzertifikate (durch entsprechende externe Anwendungen inkl. Prüfung der Personalien) gebunden werden.			akzeptabel mit Evaluation
R2- Hacker	110	(Massenhafte) Erstellung von QR-Codes (Impfnachweise/ Testzertikate) für die CWA-App	Weil die CWA-App als Wallet Funktion für die Impfnachweise konzipiert wurde, besteht keine Möglichkeit, gefälschte Impfnachweise beim Registrieren in der CWA-App zu erkennen, sofern diese den Datenstruktur-Vorgaben der CWA-App entsprechen. Die Datenstruktur-Vorgaben für die Impfzertifikate sind öffentlich verfügbar. Daher könnten (qualifizierte) Angreifer Impfnachweise inkl. QR-Code erstellen und in Umlauf bringen. Diese Impfnachweise würden von der CWA-App als valide erkannt und importiert werden. Dadurch könnte ein CWA-Nutzer dazu verleitet werden, sich mittels gefälschter Impfnachweise Freiheiten bzw. Privilegien zu erschleichen. Mit [Release 2.4] werden Testzertifikate in die CWA integriert. Ein Testcenter könnte für viele Personen negative Tests ausstellen, obwohl die Personen sich nicht testen ließen oder ein positives Testergebnis hatten. Die negativen Tests können dann auch in die CWA gelangen. Der Angreifer würde dann für das jeweilige Testergebnis ein Testzertifikat anfordern und sich so Freiheiten oder Privilegien erschleichen können.	Ja	3	3	3	3	1	1	1	1	1	3	9	VT, IG, ZB, DM	Das Gewähren von Freiheiten und Privilegien muss an eine Prüfung der in der CWA-App angezeigten Impfzertifikate (durch entsprechende externe Anwendungen inkl. Prüfung der Personalien) gebunden werden.			akzeptabel mit Evaluation
R2- Hacker	111	[Release 2.15] Gelöschte Daten führen zu Einschränkungen der fehlerfreien Arbeitsweise der CWA-App	Sofern es einem Angreifer gelingen solle, Daten aus der CWA-App zu löschen, kann die fehlerfreie Funktionsweise der CWA-App nicht sichergestellt werden. Von solch einem Angriff wäre möglicherweise auch das Feature zur Nutzung des Validierungsservices betroffen.	Ja	1	0	0	0	3	0	0	0	0	1	3	VF	Keine technischen Mitigationsmaßnahmen möglich.			

Datenschutzfolgenabschätzung (DSFA) VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	Zeilen-Nr.	Bedrohung/ Risiko	Nähere Beschreibung des Risikos	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung / Nichtverkettung	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen	geplante Maßnahmen	Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können	Restrisiko
	112	**8) Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)**																		
R1-CWA-Nutzer	113	[Release 2.11] QR-Code wird nicht erkannt/ als ungültig dargestellt	Ein CWA-Nutzer macht ein Foto von seinem QR-Code und legt es im Speicher seines Smartphones ab. Nun versucht der CWA-Nutzer, dieses Bild vom QR-Code einzulesen und in der CWA App hinzuzufügen. Allerdings wird der QR-Code nicht erkannt, weil z.B. der QR-Code unscharf auf dem Bild zu sehen ist.	Ja	2	0	0	0	1	0	1	0	0	0	2	VF, BT	CWA-Nutzer erhält Fehlermeldung und kann original QR-Code erneut einscannen.			akzeptabel
R1-CWA-Nutzer	114	(Versehentliche) Löschung von EU-weit akzeptierten Impfnachweisen nach der Auffrischungsimpfung	Sofern ein CWA-Nutzer seine Impfnachweise (1 von 2 und/oder 2 von 2) in der CWA löscht, nachdem er eine Auffrischungsimpfung erhalten hat, wäre es möglich, dass er dann keinen gültigen Impfnachweis in der CWA verfügbar hat, sofern die entsprechenden Regelwerke in der EU (des RKI) zur Akzeptanz des Auffrischungsimpfungen nicht angepasst werden.	Ja	1	1	1	1	3	1	3	1	1	1	3	VF	Änderung in der UI gemäß EU - Regeln (3/3).			akzeptabel
R1-CWA-Nutzer	115	[Release 2.13/ 2.14] (Papierkorbfunktion für Zertifikate und Test-Ergebnisse): Fehlbedienung der Papierkorbfunktion für Zertifikate	Ein CWA-Nutzer könnte sein DCC Zertifikat/ Testergebnis in den Papierkorb verschieben und die CWA-App nie wieder öffnen. Das Zertifikat würde so nicht gelöscht werden. Ein CWA-Nutzer (der die CWA-App nicht wieder nutzt) könnte annehmen, dass sein Zertifikat in den Papierkorb geschoben wurde und nach einer gewissen Zeit automatisch von seinem Smartphone gelöscht wird.	Ja	2	1	0	0	0	0	0	0	0	0	2	DM	Mit (versehentlicher/ unbefugter) Öffnung wird eine Zeitüberschreitung erkannt (länger als 30 Tage im Papierkorb) und automatisch gelöscht.			
R1-CWA-Nutzer	116	[Release 2.13/ 2.14] (Papierkorbfunktion für Zertifikate und Testergebnisse): De-Installation der CWA-App vom Smartphone	CWA-Nutzer verschiebt sein DCC Zertifikat/ Testzertifikat/ Testergebnis („aus Versehen") in den Papierkorb. Nach 30 Tagen benötigt der CWA-Nutzer sein DCC Zertifikat erneut (z.B. beim Urlaubsrückkehrer). Allerdings ist das DCC Zertifikat durch die automatische Löschfunktion des Papierkorbs nicht mehr in der	Ja	1	0	0	0	2	0	2	0	0	0	2	VF, BT	Zusätzliche Nutzung einer (analogen) Alternative. Information der CWA-Nutzer, dass Zwischenschritt über Papierkorb erfolgt und dieser automatisch geleert wird.			
R6 - Krimineller	117	Diebstahl/ ungerechtfertigte Nutzung (Kopien) von Zertifikaten im Testzentrum	Ein Angreifer stiehlt ein Zertifikat vom Testzentrum und lässt damit für sich ein Zertifikat ausstellen.	Ja	2	1	4	4	1	1	1	2	2	2	8	VT, IG	Verantwortung für Diebstahlsschutz beim PoC, Designentscheidung c.) D-2-5 (zusätzliches Datum zur Dublettenvermeidung).			akzeptabel mit Evaluation
R6 - Krimineller	118	Diebstahl/ ungerechtfertigte Nutzung von Zertifikaten im Testzentrum durch "Spearfishing"	Ein Angreifer schickt eine Person zu einer Teststelle von der er weiß, dass diese Kopien von QR-Codes verwenden. Der Angreifer überredet eine Person, sich dort testen zu lassen und versucht so, an dessen Testzertifikat zu gelangen, indem er den Test direkt in seiner App registriert, bevor das Opfer sich registrieren konnte. (Mit Mitigationsmaßnahme der Information der CWA-Nutzer, dass die Funktionalität nur für den privaten Gebrauch gedacht ist und keine Verpflichtung zum Vorzeigen an Dritte besteht (Designentscheidungen c D-3.2-2). Mithin Annahme: Angreifer hat bereits einen QR-Code und kennt das Geburtsdatum vom Opfer).	Ja	2	1	4	4	1	1	1	2	2	2	8	VT, IG	Information der CWA-Nutzer, dass die Funktionalität nur für den privaten Gebrauch gedacht ist und keine Verpflichtung zum Vorzeigen an Dritte besteht (Designentscheidungen c D-3.2-2). Hinweis an CWA-Nutzer, QR-Code möglichst unverzüglich einzucannen. Nach Scan durch Berechtigten besteht Missbrauchsrisiko nicht mehr.			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	119	Falsche Zuordnung von PCR-Testergebnissen zu Schnelltestergebnissen oder Chronologie der individuellen Testabfolge (Schnelltest/ PCR-Test/ Schnelltest…) führt zum Überschreiben von Testergebnissen.	PCR-Tests als auch Schnelltests verwenden SHA-256 Hashwerte als CWA-Test-ID. Diese IDs dienen als eine „Verbindung" zu einem Testergebnis. Im Moment sollen die PCR-Tests als auch die Schnelltests von der CWA-App vom CWA Test Result Server über den Verifikation Server durch „Polling" heruntergeladen werden. Es werden dabei die Schnelltests als auch die PCR-Tests in einer Datenbank unter den verschiedenen IDs gespeichert. Sofern bei der Erstellung der IDs gleiche IDs (Schnelltest und PCR-Test) erzeugt werden, könnte es passieren, dass das gespeicherte Testergebnis überschrieben wird. Der CWA-Nutzer würde so ein falsches Testergebnis angezeigt bekommen.	Ja	1	1	1	3	1	1	1	1	1	1	3	IG	Verwendung von Algorithmen zur Erzeugung von eindeutigen Hashcodes, die nicht zu Duplikaten führen. Die Gültigkeit der Tests beläuft sich auf maximal 14 Tage. Die Eintrittswahrscheinlichkeit von Kollisionen über UUIDs ist sehr gering. Logische Trennung von PCR und Schnelltests im Test-Result-Server (Designentscheidung c D-6-2, F-10-7) und Zugang auf das Testergebnis wird auf App - Ebene implementiert, um mögliche Überschreibungen der Daten zu verhindern.			akzeptabel
R4- Betreiber Server (T)	120	Falsche Zuordnung/ Verzerrungen hinsichtlich von Aussagewert von Schnelltests und PCR-Tests	Durch die fehlende Trennung von Schnelltests und "Labortests" von der Eingabe in den Schnelltestzentren/ Laboren bis zur Speicherung im Backend kann der Aussagewert der Testergebnisse verzerrt werden. Dies ist ein Risiko für die Integrität.	Ja	1	1	1	3	1	1	1	1	1	3	3	IG, ZB	PCR und Schnelltests bekommen unterschiedliche Wertebereiche (Designentscheidungen c.,D-6-2). Die Wahrscheinlichkeit einer Kollision bei der Erstellung von SHA-256 Werten ist sehr gering.			akzeptabel
R9 - DCC - Verifier	121	DCC-Rules: inkonsistente/ nicht-einheitliche/ veraltete Regelwerke zur Validierung der Zertifikate und deren technische Umsetzung	Sofern die Ablage der Regelwerke nicht zentral erfolgt, also alle Anwendungen, die an der Validierung beteiligt sind, möglicherweise unterschiedliche Quellen zum Laden der Regelwerke nutzten, dann wäre es möglich, dass durch Netzwerk-/ Sync-, … Probleme nicht immer die identischen Regelwerke zur Validierung genutzt werden. Das kann dazu führen, dass länderspezifische Validierungen unterschiedlich ausfallen können. Das hätte für Nutzer möglicherweise extrem negative Konsequenzen im Hinblick auf Reiseaktivitäten. Sofern die Umsetzung der Validierung der Regelwerke nicht einheitlich erfolgt, also alle Anwendungen jeweils eigenen Umsetzung des Validierungsverfahren und Regeln nutzen, dann wäre es möglich, dass es durch Unterschiede/ Fehler in der Umsetzung nicht immer zu identischen Validierungsergebnisse kommen könnte. Das kann dazu führen, dass länderspezifische Validierungen unterschiedlich ausfallen können. Das hätte für Nutzer möglicherweise extrem negative Konsequenzen im Hinblick auf seine Reiseaktivitäten.	Ja	2	1	1	3	1	1	1	3	3	2	6	IG,IV, TR	Bereitstellung von Referenzimplementierungen der Apps. Verwaltung des Lebenszyklus der DSC (Signing Certificates). Ergänzung der UI mit Datum, Gültigkeit und Alter der Validationsregelwerke. Sicherheit der länderspezifischen Upload Schnittstellen (MFA, mTLS, Audit/ Logging).			akzeptabel mit Evaluation
R8- Behörden (Verantwortliche anderer EU-Länder)	122	Fehlerhafte Signaturprüfung aufgrund von Implemeterungsfehlern	Sollte es zu Fehlern in der Implementierung einer oder mehrere an dem Prüfprozess beteiligten Komponenten (auch in anderen EU-Ländern) kommen, kann dies dazu führen, dass es beim Hinzufügen von Zertifikaten bzw. bei deren Überprüfung zu Fehlern kommen kann. Sofern es bei der Signaturprüfung zu einem Fehler kommen sollte, könnte die CWA-App dem CWA-Nutzer das entsprechende Zertifikat fälschlicherweise als gültig/ ungültig anzeigen; es könnte fälschlicherweise zur Zurückweisung eigentlich gültiger Zertifikate kommen bzw. fälschlicherweise zur Anerkennung eigentlich ungültiger Zertifikate.	Ja	2	1	1	3	3	1	3	1	1	1	6	IG, VF, RE	Bereitstellung von Referenzimplementierungen der Apps. Verwaltung des Lebenszyklus der DSC (Signing Certificates). Ergänzung der UI mit Datum, Gültigkeit und Alter der Validationsregelwerke. Sicherheit der länderspezifischen Upload Schnittstellen (MFA, mTLS, Audit/ Logging).			akzeptabel mit Evaluation
R8- Behörden (Verantwortliche anderer EU-Länder)	123	Fehlerhaft erkannte "technische Gültigkeitsdauer" des Digital Signing Certificate (DSC)	Sofern es bei der Zertifikatsprüfung zu einem Fehler bei der Ermittlung der technischen Gültigkeitsdauer des DSC kommen sollte, kann dies dazu führen, dass dem CWA-Nutzer ein ungültiges Zertifikat in der CWA-App anzeigt wird, obwohl das DSC noch gültig ist bzw. ein gültiges Zertifikat, obwohl das DSC ungültig ist.	Ja	2	1	1	3	3	1	3	1	1	1	6	IG, VF, RE	Bereitstellung von Referenzimplementierungen der Apps. Verwaltung des Lebenszyklus der DSC (Signing Certificates). Ergänzung der UI mit Datum, Gültigkeit und Alter der Validationsregelwerke. Sicherheit der länderspezifischen Upload Schnittstellen (MFA, mTLS, Audit/ Logging).			akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	124	Fehlerhafte Anzeige der Gültigkeit von Zertifikaten aufgrund lokaler Zeit- oder Datumsumstellung	Die Überprüfung der technischen Gültigkeit und der Validationsregeln wird basierend auf dem lokal konfigurierten Datum und der Uhrzeit durchgeführt. Ein falsch konfiguriertes Datum oder Uhrzeit auf den lokalen Geräten könnte zu irrführenden Anzeigen der Zertifikatsgültigkeiten führen.	Ja	1	1	1	3	3	1	3	1	1	1	3	IG, VF, RE	Anzeige in der CWA-App, wann die Verifizierung stattgefunden hat (Vorbehalt).			akzeptabel
R2- Hacker	125	DNS-Spoofing / Man-in-the-Middle Attacke: Kommunikation der PoCs statt mit einem Server eigener Wahl statt mit dem PoC-Backend (Vorgetäuschter Server)	Durch DNS-Spoofing oder eine Man-in-the-Middle Attacke könnte ein Angreifer die PoC dazu bringen, statt mit den legitimen Servern mit einem Server seiner Wahl zu kommunizieren. Das betrifft auch den PoC-Server der Testzentren. Durch Senden unzulässiger oder gefälschter Inhalte könnte der Angreifer die Funktion der PoC beeinträchtigen oder gar zum Erliegen bringen.	Ja	1	0	0	0	4	4	4	4	4	4	4	VT, DM, ZB, T , IV	Designentscheidungen a. B-1-5ff. Einsatz von mutual-TLS.			akzeptabel
R2- Hacker	126	Denial of Service (Mutwillige Überlastung) Angriffe auf CWA-Komponenten über Schnelltest-Netzwerk-Schnittstellen	Die Netzwerk-Schnittstellen sind mit mutual-TLS geschützt und weitere DDoS-Angriffsversuche werden durch den Anti-DDOS der OTC abgewehrt (Verfügbarkeitsrisiko).	Ja	1	0	0	0	3	0	3	0	0	3	3	VF, R, ZB	AV-Verträge mit DL, inkl. TOM , Designentscheidungen D-11-1 (Einsatz von Anti-DDoS Gegenmaßnahmen für die Schnelltest-Netzwerk-Schnittstellen).			akzeptabel

Datenschutzfolgenabschätzung (DSFA)
VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)

				Risikobewertung															
						Schadensausmaß													
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R2- Hacker	127	Speicherung von pD im Rahmen der DCC-Records über die Gültigkeitsdauer von Testzertifikaten hinaus	Schnelltestzentren (etwa Flughafen) können ihre Schnelltest-Anbindung an die CWA nicht nutzen, wenn die Schnelltestsanbindung an das PoC-Backend nicht verfügbar ist.	Ja	3	0	0	0	3	0	3	0	0	3	9	VF, R, ZB	Verantwortung der PoC und Drittanbieter, auch ihre Systeme ausreichend gegen DDoS-Angriffe zu schützen.			akzeptabel mit Evaluation
R2- Hacker	128	Denial of Service Angriffe (Regelwerk für Zertifikate und Signaturüberprüfungsdaten)	Der CWA-Server lädt sich die notwendigen Daten zur Validierung der Signaturen einer öffentlichen Komponente außerhalb der CWA herunter. Sollte es einem Angreifer gelingen, die Daten in dieser Quelle zu modifizieren oder zu löschen, lädt sich der CWA-Server von einem Angreifer modifizierte Daten herunter und stellt diese den CWA-Apps über das CDN zur Verfügung. Sollten diese nun die modifizierten Daten bei der Signaturprüfung verwenden, könnte es zu einem Denial-of-Service einiger Funktionen innerhalb der CWA-App kommen. Sofern es einem Angreifer gelingen sollte, die notwendigen Daten zur Signaturüberprüfung mittels CWA auf dem CDN (insbesondere die DSC) zu modifizieren/löschen, dann kann der CWA-Nutzer seine gültigen Zertifikate nicht in die CWA hinzufügen obwohl diese gültig wären.	Ja	1	0	0	0	3	0	3	0	0	3	3	VF, RE, ZB	Schutz der Distributionsschnittstellen (CDN) gegen DDoS-Angriffe.	Einsatz von Digitalen Signaturen und ggf. Versionierung für DSC-Listen und Regelwerke.		akzeptabel
R2- Hacker	129	[Release 2.15] Denial-of-Service Angriff auf die Netzwerkverbindung/ Datenvolumen des CWA-Nutzers durch die Übertragung sehr großer Datenmengen	Durch das Übertragen von großen Datenmengen an die CWA-App könnte das Datenvolumen des CWA-Nutzers aufgebraucht werden.	Ja	3	0	0	0	3	0	3	1	0	1	9	VF, BT		Paketgrößenlimitierung in der CWA, soweit möglich (in Prüfung/ Planung).		akzeptabel mit Evaluation
R4 - Softwareentwickler / SAP	130	[Release 2.15] Fehlerhalfte Update-Mechanismen der eTag's (Denial-of-Service Angriffe)	Wenn die Allow-List, die die CWA-App vom CDN erhält, in irgendeiner Weise beschädigt ist und die Allow-List auf dem CDN kein neues eTag enthält, ruft die CWA keine neue Allow-List ab, wenn sie bereits eine im Cache hat (auch wenn diese beschädigt ist). Dies kann zu einem Denial-of-Service des DCC-Validierungsservice führen, bis eine neue Allow-List veröffentlicht und an den CWA-Client verteilt wird.	Ja	1	0	0	3	3	0	0	0	0	1	3	IG, VF	Standard TOM CDN.			
R4- Testcenter	131	Nicht ausreichende Sicherheit für Mandanten, die ihre Ergebnisse über den Proxy in die CWA hochladen		Ja	1	0	1	2	1	1	1	1	1	1	2	IG	TOM (Absicherung der Kommunikation durch Einsatz von mTLS, whitelisting).			akzeptabel
R2- Hacker	132	Mutwillige Überlastung über QR-Code ("ZIP-Bombe")	Die enthaltenen Informationen auf dem QR-Code werden zwecks Ressourcenoptimierung komprimiert. Ein Angreifer könnte eine sogenannte Archivbombe erstellen und diese in einem schädlichen QR-Code einpacken. Beim Entkomprimieren der Archivbombe werden die lokalen Ressourcen der QR-Code-Leser ausgeschöpft. (Ein Beispiel für eine Archivbombe ist die Datei 42.zip: mit einer komprimierten Größe von 42 kB beim Entpacken werden insgesamt Dateien in einer Größe von 4,5 PetaBytes entpackt).	Ja	1	0	0	0	1	0	1	0	0	0	1	VF, BT	Maximale Größe wurde (10 MB) für die dekomprimierte Information (DSK CWA App v2.3, 7.4.17.3.1) wurde definiert.			akzeptabel
R1-CWA-Nutzer	133	[Release 2.15] Eingeschränkte/ Fehlende Funktionen der CWA-App aufgrund mangelnder Rechenleistung der im Smartphone verbauten CPU	Sofern die Rechenleistung der CPU des vom CWA-App-Nutzer verwendeten Smartphones nicht ausreichend ist, kann es z.B. beim Generieren der lokalen Schlüssel zu Problemen kommen, die möglicherweise zu Fehlern in der CWA-App führen. Davon könnten auch andere Anwendungen betroffen sein, die auf dem Smartphone des Nutzers laufen.	Ja	2	0	0	0	2	0	0	0	0	1	4	VF	Keine technischen Mitigationsmaßnahmen möglich; Verantwortung der CWA-Nutzer.			
R4- Betreiber Server (T)	134	[Release 2.15] Nicht ausreichend skalierender "Distribution Service"	Für die Verteilung der Daten an das CDN wird der "Distribution Service" genutzt. Sofern es absichtlich oder unabsichtlich zu einem sehr hohen Aufkommen an Service-Anfragen für diesen Service kommen sollte, könnte dies zu einer Überlastung und ggf. sogar zu einem Ausfall des "Distribution Service" führen. Das könnte möglicherweise auch Einfluss auf die korrekte Funktionsweise der CWA-Anwendung haben.	Ja	1	0	0	0	3	0	0	0	0	1	3	VF	Angemessene Behandlung von Ausnahmefällen, Bereinigung von Eingaben, Überwachung (job runtime).			
R4 - Softwareentwickler / SAP	135	Versehentliche/ absichtliche Sperrung gültiger Zertifikate	Falls es bei der Konfiguration/ Überprüfung der zu widerrufenenden Identifier, z.B. AusstellerID, zu einem Fehler kommen sollte (z.B. Tippfehler), dann besteht die Möglichkeit, dass ein anderer, eigentlich gültiger Identifier als ungültig in der CWA-App markiert wird.	Ja	2	1	1	3	3	1	1	1	1	1	6	IG, VT			Der Prozess sollte optimiert werden, um die Fehleranfälligkeit weiter zu reduzieren	akzeptabel mit Evaluation
R4- Betreiber Server (T)	136	[Release 2.15] Versehentliche/ absichtliche Manipulation Allow-List	Die Allow-List wird manuell gepflegt. Hier können auf 2 Arten Manipulationen der Einträge erfolgen. (1) Sofern ein Mitarbeiter sowohl Zugriff auf die "privaten" als auch die "öffentlichen" Schlüssel des Backends haben sollte, könnte er die Allow-List abändern und die abgeänderte Allow-List über das CWA publizieren und damit an die CWA-Nutzer verteilen.(2) Andererseits werden die Hinweise zu manueller Pflege der Einträge in dieser Liste mittels E-Mail an die beteiligten Partner kommuniziert. Die Anpassung der Einträge in der Liste erfolgt dann manuell. Durch die fehlende Prozessautomatisierung ergeben sich diverse Risiken, z.B. •Manuelle Manipulation der Liste durch einen Innentäter •Fehlerhafte manuelle Anpassungen durch Tippfehler •Zeitverzug bei der Umsetzung der Anpassungen •Die Nutzung unsicherer Mailsysteme könnte einen Angriff zur Manipulation der Allow-List erleichtern.	Ja	2	0	3	3	0	0	0	0	0	1	6	VT, IG		Zu Risikobeschreibung (2): Nutzung sicherer "signierter" Mails für die Kommunikation		
R2- Hacker	137	[Release 2.15] Ausweitung von Berechtigungen aufgrund von Erpressungsmails	Sofern Personen mit entsprechenden Berechtigungen durch Erpressungsmails unter Druck gesetzten werden sollten, könnten diese Mitarbeiter vom Angreifer dazu genötigt werden, neue Allow-List-Einträge zu erstellen, bestehende Allow-List Einträge zu löschen, die öffentlichen-Schlüssel des CWA-Servers zu verändern. So könnten gewisse Schritte, die zur Absicherung des Prozesses zur Änderung der Allow-List vorgesehen sind (z.B. Peer-Review), umgangen werden.	Ja	1	0	3	3	0	0	0	0	0	1	3	VT, IG	Rollenkonzept			
R2- Hacker	138	[Release 2.15] Verlust/ Weitergabe des "privaten Schlüssels"	Sofern der private Schlüssel, mit dem die Daten in der Allow-List auf GitHub signiert werden, verloren oder auf andere Wege bekannt wird, könnte ein Angreifer diesen Umstand nutzen, um seine eigene signierte Allow-List zu erstellen. Sollte er in den Besitzt des privaten Schlüssels gelangt sein, besteht die Möglichkeit, dass dieser die Daten in der Allow-List modifiziert. Wenn ein Angreifer Zugriff auf den privaten Schlüssel hat oder den öffentlichen Schlüssel ersetzen kann und dann die Allow-List manipuliert, könnten alle durchgeführten Änderungen unbemerkt bleiben.	Ja	1	0	0	3	0	0	0	0	0	1	3	IG	Implementierung eines Secure Key Managements.			
R2- Hacker	139	[Release 2.15] Nichtnutzbarkeit/ Nichtverfügbarkeit der Allow-List	Sollte die Allow-List wegen eines Ausfalls des Github-Systems, des Internets, eines oder mehrerer der beteiligten Mailserver, Ausfall des CDN' oder wegen sonstiger technischer Fehler/ Probleme nicht gepflegt und verteilt werden können, dann entspräche dies einem „Denial-of-Service" der Allow-List. Diese könnte dann – ebenso wie notwenige Anpassungen der Liste – nicht mit den richtigen Inhalten über das CDN an die CWA-Nutzer verteilt werden.	Ja	2	0	0	0	2	0	0	0	0	1	4	VF	Etablierung eines redundanten Prozesses.			

Datenschutzfolgenabschätzung (DSFA) VT 6: Schnelltest-Anbindung + Schnelltest-Profil + Nachweisfunktion + Anzeige Impfzertifikate (Wallet Funktion) + Integration von Testzertifikaten (Wallet Funktion) + Genesenenzertifikat (Wallet) Funktion + Funktion für Familienzertifikate + DCC-Validation Rules + Auffrischungsimpfung + Druckfunktion+Universal QR-Code Scanner + Papierkorbfunktion für Zertifikate + Widerrufsfunktion für Zertifikate + Integration Validation Service (Stand: 10.12.2021)				Risikobewertung																
						Schadensausmaß														
Risiko-Quelle	**Zeilen-Nr.**	**Bedrohung/ Risiko**	**Nähere Beschreibung des Risikos**	**Schwachstelle (ja/nein)**	**EW**	**Datenminimierung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Authentizität**	**Resilienz**	**Intervenierbarkeit**	**Transparenz**	**Zweckbindung / Nichtverkettung**	**Risikoklasse**	**Soll-Maßnahmen - ID**	**(etablierte) Maßnahmen**	**geplante Maßnahmen**	**Bewertung, warum insbesondere "rote" Risiken akzeptiert werden können**	**Restrisiko**
R2- Hacker	140	[Release 2.15] Manipulation des privaten Krypto-Schlüssels	Sofern der private Schlüssel zum Signieren der Allow-List manipuliert werden sollte, wäre die in der CWA-App hinterlegten Allow-List nicht mehr nutzbar. Zudem könnte ein manipulierter oder beschädigter Schlüssel zu einer anfälligen Krypto-Bibliothek die Ausführung von Code in der CWA-App ermöglichen.	Ja	1	0	0	3	0	0	0	0	0	1	3	IG	Implementierung eines Secure Key Managements, Durchführung von Peer Review und Sichestellung geteilter Verantwortungen (Rollenmanagement). Durchführung von Eingabevalidierungen des Encryption Key, Durchführung von Sicherheitsscans von Open-Source-Software.			
R2- Hacker	141	[Release 2.15] Manipulation der Allow-List durch eine Sandbox-Schwachstelle	Sofern die Sandbox vom Betriebssystem nicht hinreichend geschützt ist, wäre es einem Angreifer möglich, die Allow-List zu manipulieren. Dadurch könnte die CWA-App mit einem nicht genehmigten Validierungs-Service-Provider kommunizieren. Sollte es dem Angreifer gelingen, die Sandbox zu umgehen und die Daten zur Allow-List aus der CWA App zu löschen/ manipulieren, dann könnte die CWA-App möglicherweise nicht mehr den Buchungs-/ Validierungsprozess nutzen.	Ja	1	0	0	3	0	0	0	0	0	1	3	IG	Validierung der Allow-List-Signatur bei jeder Nutzung.			
	142	**9) Verarbeitung über die Speicherfrist hinaus**																		
R4- Betreiber Server (T)	143	Speicherung von pD im Rahmen der DCC-Records über die Gültigkeitsdauer von Testzertifikaten hinaus	Art. 9 Abs. 3 der DCC-I-VO bestimmt, dass die zur Ausstellung verwendeten personenbezogenen Daten nicht länger gespeichert werden dürfen, als das DCC selbst gültig ist. Die Nachverfolgung von Missbräuchen, etwa die Ausstellung von unrichtigen Zertifikaten durch Testzentren, ist für die IT-Forensik in dieser kurzen Zeitspanne nicht gewährleistet. Es droht die Verletzung des Grundsatzes der Datenminimierung und Speicherbegrenzung.	Ja	2	3	1	1	1	1	1	3	3	3	6	DM, IV, TR, ZB	Festlegung von Aufbewahrungspflichten in Abstimmung mit der verantwortlichen Stelle. Erstellung eines Löschkonzepts (Designentscheidungen c.) D-9-5c).			akzeptabel mit Evaluation
R4- Betreiber Server (T)	144	Unbefristete Speicherung von Daten (inkl. Metadaten) auf CWA-Server und mögliche spätere Verkettung mit anderen personenbezogenen Daten		Ja	1	4	1	1	0	0	0	3	3	4	4	DM, ZB	Designentscheidungen a. D-11-1/ AVV mit DL inkl. TOM; DSK_Rahmenkonzept Kap. 14.20.2 (Das Löschen von Positivschlüsseln auf der Datenbank des CWA Servers sowie auf dem Objectstore, der als Übergabemedium zum CDN-Magenta dient, erfolgt mit den vom jeweiligen Speicherservice angebotenen Mitteln. Ein Ausnullen der betroffenen Speicherbereiche wird nicht vorgenommen). Siehe auch Aufführungen zur Löschung in den Teil-DKS, Designentscheidungen a. (D-8-1ff) und AVV inkl. TOM.			akzeptabel
R4- Betreiber Server (T)	145	Unbefristete Speicherung unrichtiger/ negativer/ nicht-notwendiger Daten		Ja	1	4	4	4	0	0	4	2	4	4	4	DM, ZB	AV-Verträge mit DL inkl. TOM , Designentscheidungen D-11-1.			akzeptabel
R10 - Validation Service Provider/ Leistungsanbieter	146	[Release 2.15] Verarbeitung von personenbezogenen Daten über den Zeitraum der berechtigten Datenverarbeitung hinaus.		Nein											-			Die Datenverarbeitung erfolgt außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA. Die Mitigationspflicht trifft die dortigen Verantwortlichen.		
	147	10) Risiken durch Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt																		
R8- Behörden (Verantwortliche anderer EU-Länder)	148	Fehlende Regelwerke zur Gültigkeit von Auffrischungsimpfungen	Fehlinterpretationen und Unklarheiten, was mit Auffrischungsimpfungen erlaubt ist und was nicht, können zur unberechtigten Einschränkungen oder unnötigen Selbstbeschränkungen führen.	Ja	3	1	3	1	1	1	1	3	3	3	9	IG, IV, TR, ZB		Empfehlung: Keine Zertifikate auf der App löschen. Auf EU-Ebene ein einheitliches Vorgehen für die verschiedenen Booster Impfszenarien entwickeln.		akzeptabel
R8- Behörden	149	Zukünftige Änderungen der DCC-Validierung sind noch nicht antizipiert und die bisherige Lösung der CWA zum Widerruf von Zertifikaten könnte durch Regelungen auf europäischer Ebene überholt werden.	Zum Teil sind Anforderungen der DCC-VO und in dieser ermöglichte Funktionen noch nicht umgesetzt. Spezifikationen auf EU-Ebene können Änderungen der Datenverarbeitung erfordern.	Ja	3	1	1	3	3	1	1	2	2	2	9	IG		Die Datenverarbeitung der CWA muss ev. an die europäischen Regelungen angeglichen werden. Der Angleich an europ. Regelungen von Diensten außerhalb der CWA muss von den jeweiligen Verantwortlichen erfolgen.		akzeptabel mit Evaluation
R8- Behörden	150	Ausweitung der in die CWA-App integrierten Funktionen (Neubewertung mit [Release 2.15])	Die Integration des Validationservices in die CWA könnte über die bisherigen Zwecke der Verarbeitung in der CWA hinausgehen.	Ja	3	3	0	0	0	0	0	0	0	3	9	DM, ZB		Die Bereitstellung eventuell erforderlicher Informationen für die Feststellung der Zweckverfolgung obliegt den Verantwortlichen der Datenverarbeitung außerhalb des Verantwortungsbereichs der verantwortlichen Stelle der CWA, soweit die Verarbeitung durch diese erfolgt.		akzeptabel mit Evaluation
R8- Behörden	151	Diskriminierung von Personen, denen die CWA-Nutzung nicht möglich ist bzw. die keinen Zugang zu Impfzertifikaten haben	Minderjährige unter 16 Jahre können die CWA nicht nutzen und haben aktuell auch keinen Zugang zu Impfstoffen. Sie haben daher auch nicht die Möglichkeit, sich „Freiheiten" mittels der CWA-Infrastruktur zurückzuholen. Es droht daher, Diskriminierungen dieser Personengruppen beim Zugang zu (öffentlichen) Einrichtungen, Veranstaltungen zu verstetigen.	Ja	3	0	0	0	3	0	0	0	0	0	9	VF		Gesamtstrategie zur Pandemiebekämpfung mit Strategie zur Sicherung von Freiheitsgewinnen auch für diese Personengruppe erarbeiten.		akzeptabel mit Evaluation