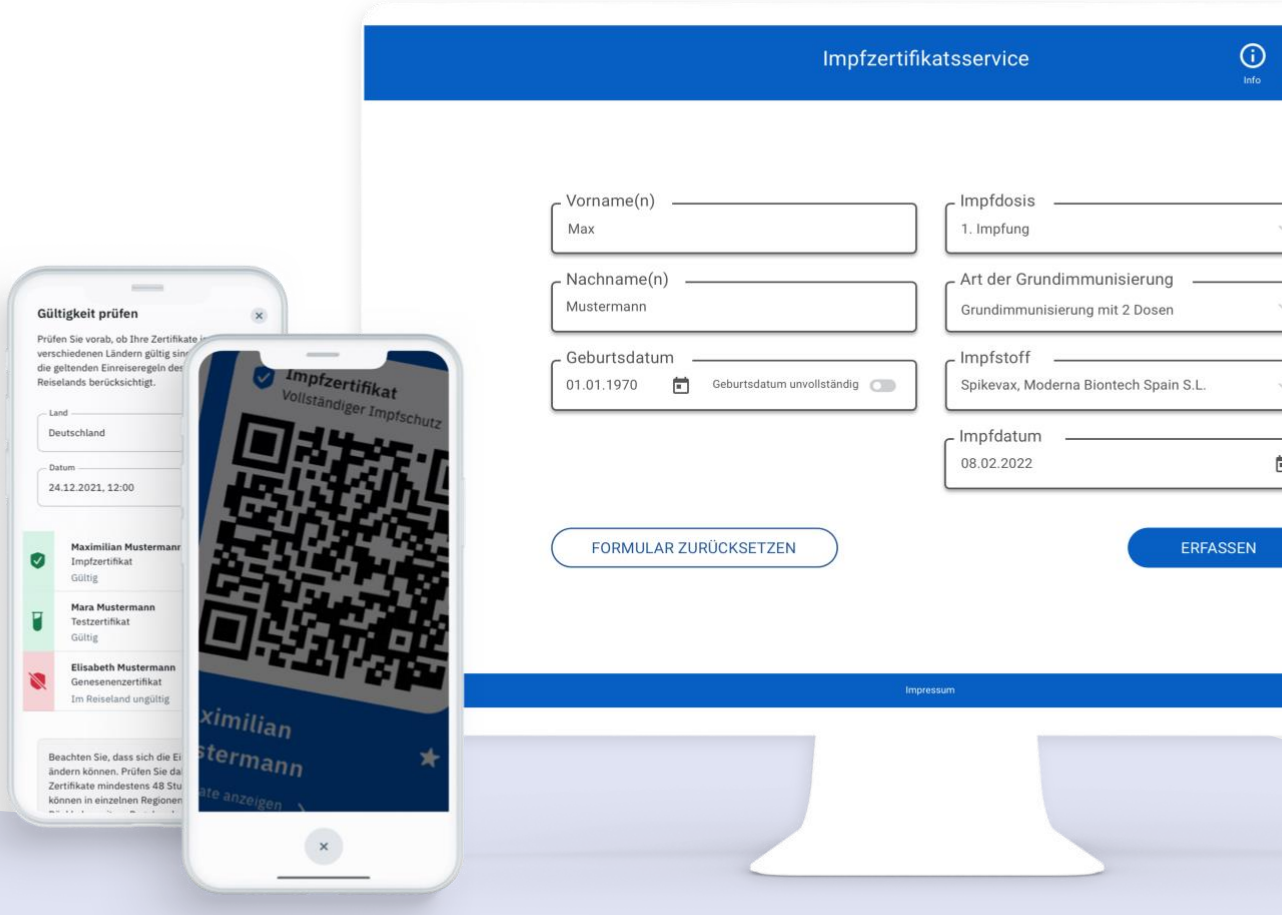
Version 1.0.1
Stand 23.12.2022

# Impfzertifikatsservice

## Nutzungshinweise und Sicherheitsempfehlungen




ROBERT KOCH INSTITUT

**Zielgruppe: Alle Anwender, Nutzer und Integratoren des Impfzertifikatsservice**

Dem Robert Koch-Institut („RKI“) obliegt gemäß § 22 IfSG die Aufgabe der technischen Generierung von COVID-19-Zertifikaten, die auf Wunsch der betroffenen Person von einer zur Erstellung des gewünschten COVID-19-Zertifikats verpflichteten Stelle ausgegeben werden.

Zu diesem Zweck stellt das RKI den zur Erstellung von COVID-19-Impfzertifikaten (§ 22 Abs. 5 IfSG) und COVID-19-Genesenenzertifikaten (§ 22 Abs. 7 IfSG) verpflichteten Stellen einen kostenlosen Onlinedienst zur Verfügung, an den diese zur Erfüllung ihrer gesetzlichen Pflicht die zur Erstellung der jeweiligen COVID-19-Zertifikate notwendigen Daten sicher an das RKI übermitteln können („Impfzertifikatsservice“). Das RKI verarbeitet im Rahmen des Impfzertifikatsservice diese Daten zur technischen Generierung der angeforderten COVID-19-Zertifikate und stellt sie der zur Erstellung verpflichteten Stelle zum Abruf bereit.

Der Impfzertifikatsservice umfasst eine über das Netz der Telematikinfrastruktur erreichbare Web-Anwendung unter https://web.impfnachweis.info/ („Web-Anwendung“) und eine Programmierschnittstelle für Betreiber von integrierten Softwarelösungen („Impfzertifikats-API“).

Die nachfolgenden Nutzungshinweise sind als Handlungs- und Maßnahmenempfehlungen zur Gewährleistung der eigenverantwortlichen, datenschutzkonformen Nutzung des Impfzertifikatsservice durch die Anwender zu verstehen. Die Beachtung dieser Nutzungshinweise liegt im eigenen Interesse der Anwender.

## I. Allgemeines

„Anwender“ im Sinne dieser Nutzungshinweise sind

- Betreiberinnen und Betreiber von zur Ausgabe von COVID-19-Zertifikaten verpflichteten Stellen („Zertifizierungsstellen“) und
- Betreiberinnen und Betreiber von integrierten Softwarelösungen („Integratoren“).

Zur Nutzung des Impfzertifikatsservice sind ausschließlich die Anwender und die von den Anwendern eingesetzten Mitarbeiter („Nutzer“) berechtigt. Ein Anspruch auf Zulassung zur Nutzung des Impfzertifikatsservice besteht nur im Rahmen der gesetzlichen Bestimmungen.

Die technischen und organisatorischen Voraussetzungen und die notwendigen Einrichtungsschritte für die Anbindung und Nutzung des Impfzertifikatsservice sowie etwaige Nutzungsbedingungen werden dem Anwender unter https://digitaler-impfnachweis-app.de/ im Bereich „Materialien zum Download“ und auf Anfrage erläutert.

Die Anwender sind für die von ihnen durchgeführte Datenverarbeitung datenschutzrechtlich eigenständig verantwortlich. Für sämtliche Verstöße gegen datenschutzrechtliche Bestimmungen durch die Nutzer des Anwenders im Zusammenhang mit der Nutzung des Impfzertifikatsservice übernimmt der Anwender die volle Verantwortung.

Der Impfzertifikatsservice darf ausschließlich im Rahmen der geltenden Gesetze verwendet werden. Eine wissentliche Ausstellung von unrichtigen COVID-19-Zertifikaten zu Täuschungszwecken (beispielsweise durch Ausstellung eines Impfzertifikats für eine nicht geimpfte Person) stellt gemäß § 75a Abs. 1 IfSG eine Straftat dar und kann mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden.

## II. Empfohlene Kernmaßnahmen für alle Anwender

- Der Anwender wird das RKI über Sicherheitsvorfälle (z. B. Verlust von Authentifizierungsmedien, unbefugte Zugriffe auf X.509-Zertifikate oder Bekanntwerden von Zugangsdaten) unverzüglich informieren. Dies gilt entsprechend auch bei schwerwiegenden sicherheitstechnischen Störungen, bei Verletzungen von

Vorschriften zum Schutz personenbezogener Daten, sonstigen Unregelmäßigkeiten bei der Nutzung des Impfzertifikatsservice sowie entsprechenden konkreten Verdachtsfällen.

- Das RKI kann bei Sicherheitsvorfällen unter
  - aussteller-support@covpass-app.de

  informiert werden.

- Es erfolgt eine angemessene Aufklärung der Nutzer des Anwenders zum Umgang und zur Verwendung von Authentifizierungsmedien oder Zugangsberechtigungen. Der Anwender implementiert einen Prozess zur Einrichtung, Ausgabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen an die von ihm beauftragten Nutzer.
- Authentifizierungsmedien und Zugangsdaten dürfen unbefugten Personen nicht zugänglich gemacht werden. Die Nutzer sind entsprechend zu sensibilisieren.
- Wenn ein Nutzer oder der technische Verantwortliche auf Seiten des Anwenders ausscheidet oder einen anderen Aufgabenbereich erhält, werden sämtliche dieser Person zugänglichen Authentifizierungsmedien und Zugangsberechtigungen hinsichtlich aller nicht mehr in seinem Aufgabenbereich liegenden Systeme mit Zugang zum Impfzertifikatsservice unverzüglich entzogen.
- Der Anwender beachtet die Installations- und Nutzungsanleitungen des RKI. Diese sind zu finden unter https://web.impfnachweis.info/ in den Bereichen „Technische Details“ und „Materialien zum Download“.

## III. Empfohlene Richtlinien für Nutzer

Der Anwender verpflichtet die Nutzer zur Einhaltung folgender Sorgfalts- und Mitwirkungspflichten:

- Der Nutzer hat sicher zu stellen, dass keine unberechtigte Person Zugriff zum Computer erhält, mit dem die Zertifikate ausgestellt werden.
- Der Nutzer muss durch ein Passwort den Computer schützen und bei Verlassen des Arbeitsplatzes den Sperrbildschirm des Computers aufrufen. Zudem muss der Zugang räumlich eingeschränkt werden.
- Eine Weitergabe von Zugangsdaten (z.B. Passwörtern) ist nicht zulässig.
- Beim Einsatz von mobilen Einrichtungen (z. B. Impfbusse) werden die dort tätigen Nutzer zur Einhaltung von angepassten Sorgfalts- und Mitwirkungspflichten verpflichtet, die den spezifischen Risiken der betreffenden mobilen Einrichtung (z. B. erhöhtes Diebstahlrisiko, Verfügbarkeitsrisiken durch gestörte Internetverbindung) gerecht werden.
- Der Zugang muss über sichere Netzwerke erfolgen (z.B. kein öffentliches W-LAN).
- Der Verlust eines Computers, das Bekanntwerden von Zugangsdaten, die Entdeckung von Missbrauch oder sonstige sicherheitsrelevante Vorfälle sind vom Nutzer unverzüglich dem Anwender zu melden.
- Es muss durch den Anwender und dem Nutzer sichergestellt sein, dass durch unsachgemäße Nutzung keine Schadsoftware auf den Computer gelangt.

## IV. Spezielle Richtlinien bei der Benutzung von "Funktionsaccounts" im Impfzentrum

- Ein Funktionsaccount ist ein Account, der nicht einem Nutzer oder einem Gerät (Computer) sondern einer Nutzergruppe zugeordnet ist.
- Zu Schichtbeginn und Schichtende sind durch den Technischen Ansprechpartner jedem Impfmitarbeiter ein Funktionsaccount für den Zugang zum Impfzertifikatsservice zuzuweisen und ein FIDO2-Token auszugeben bzw. die Rückgabe festzuhalten.
- Die Belehrung zur Nutzung des Impfzertifikatservice durch den Impfzentrumsleiter oder Technischen Ansprechpartner sollte nachvollziehbar protokolliert und durch Unterschrift des Nutzers bestätigt werden.

- Wenn der Impfzentrumsmitarbeiter den Arbeitsplatz (z.B. für eine Pause) verlässt, ist neben der Abmeldung am Computer auch der FIDO2-Token vom Computer abzuziehen und sicher vor unbefugten Zugriffen zu verwahren.
- "Springer", die parallel zu einer regulären Schicht in Pausen einspringen, erhalten ihren eigenen Funktionsaccount und FIDO2-Token zur Anmeldung an den Arbeitsplätzen. Es gelten die gleichen Vorgaben wie für Impfzentrumsmitarbeitende mit Funktionsaccount.
- Die Anzahl der Funktionsaccounts (inkl. Token) MUSS der max. Schichtgröße (inkl. Springer) entsprechen.
- Die Passwörter der Funktionsaccounts sind bei Schichtwechsel durch den Technischen Ansprechpartnerüber den Link auf dem Login-Screen zurück zu setzen und neu zu erstellen (keine Weitergabe von Passwörtern). Pro Funktionsaccount ist eine eindeutige E-Mail-Adresse notwendig (wenn nicht anders möglich, und unter gewissen Rahmenbedingungen, sind auch E-Mail-Aliase über ein Catch-All-Postfach möglich, auf das der Technische Ansprechpartner Zugriff hat).
- Ein FIDO2-Token sollte genau einem Account Impfzentrumsmitarbeiter zugeordnet sein und wird vom Technischen Ansprechpartner von Schicht zu Schicht weitergegeben.
- Nachdem der Technische Ansprechpartner am Tagesende alle FIDO2-Token wieder in Empfang genommen hat, hat er über die Benutzerverwaltung die Funktionsaccounts zu deaktivieren und initiiert damit implizit die Zurücksetzung der Passwörter (und FIDO2-Token-zuordnung)
- Am Folgetag aktiviert der Technische Ansprechpartner entsprechend der aktuellen Schichtgröße die notwendige Anzahl der eingerichteten Funktionsaccounts erneut.
- Bei der Erstanmeldung der Impfzentrumsmitarbeiter zum Schichtbeginn wählen diese ein persönliches Kennwort und registrieren - sofern notwendig - das erhaltene FIDO2-Token mit dem Funktions-Account
- Der Technische Ansprechpartner trägt die Verantwortung, dass die oben stehenden Richtlinien eingehalten werden.
- Dem Impfzentrumsmitarbeiter wird bei Schichtbeginn ein Handzettel ausgehändigt, auf dem die wichtigsten sicherheitstechnischen Punkte und Verfahrensanweisungen verständlich beschrieben sind.

## V. Richtlinien für Integratoren

- Die Authentifizierung gegenüber der API erfolgt durch ein mTLS-Zertifikat. Der Zugang zum mTLS-Zertifikat durch unberechtigte Personen muss durch vom Integrator festgelegte und umgesetzte geeignete technische und organisatorische Maßnahmen ausgeschlossen werden. Die Einhaltung der technischen und organisatorischen Maßnahmen muss durch den Integrator jederzeit nachweisbar sein.
- Das mTLS-Zertifikat ist ausschließlich für die Verwendung in einer sicheren Rechenzentrumsumgebung vorgesehen. Das mTLS-Zertifikat darf nicht in die Client-Software der Endanwender:innen integriert werden.
- Für Prozesse, Anwendungen und Rechenzentrumsumgebungen liegen hinreichende Informationssicherheits- und Datenschutzkonzepte vor, z.B. Zertifizierung nach ISO27001. Der Zugang zu den Computern von denen die Verbindung ins Integrator-Backend hergestellt wird, ist entsprechend zu beschränken und zu überwachen.
- Es liegt eine eindeutige ID (z.B. DIM, BSNR) vor, mit der jede Lokation in der die Software angeboten wird, eindeutig identifiziert werden kann. Durch den Integrator ist sicher zu stellen, dass der identifizierte Ansprechpartner jeder Lokation auch die fachliche Berechtigung zur Anbindung besitzt (z.B. Zulassung als Betriebsarzt). Die Verantwortung hierfür liegt beim Integrator. Der Integrator hat die von ihm verwendeten eindeutigen IDs beim Betreiber vor Benutzung freigeben zu lassen. Dies gilt auch für jede nachträgliche Änderung (zusätzliche IZs, Apotheken...)
- Es wird eine Multi-Faktorauthentifizierung für die Authentifizierung gegenüber dem Integrator-Backend verwendet, über die jede/r Nutzer:in eindeutig identifiziert werden kann, d.h. es werden personalisierte Accounts und keine Funktionsaccounts verwendet. Falls ein Nutzer nicht eindeutig identifiziert werden kann, muss organisatorisch eine Verknüpfung zwischen Funktionsnutzer und realer Person hergestellt werden.

- Bei jeder Anfrage über die Impfzertifikats-API wird eine einzigartige Transaktionsnummer (im Header als X-Transaction-Id) mitgeliefert, die auf der Seite des Integrators mit dem anfordernden Nutzer eindeutig zuordenbar gespeichert wird (auditierbares Logging).
- Jeder Integrator hat vorab zu benennen, für welche Anzahl an Nutzern und welchen Nutzerkreis (z.B. Betriebsärzte, Apotheke etc.) die Lösung eingesetzt werden soll. Eine Änderung dieses Nutzerkreises ohne vorherige Absprache mit dem RKI (0800-4747-003 oder per Mail an maussteller-support@covpass-app.de) ist unzulässig (z.B. dürfen bei einem Integrator für Gesundheitsämter nicht ohne vorherige Rücksprache Zugänge für Apotheken eingerichtet werden).