SWISS COVID CERT APP

ARCHITEKTUR-DOKUMENTATION

Kompakte, bewertungsorientierte Dokumentation für Unterricht und Präsentation

VERSION: 1.1
DATUM: 05,11.2025
AUTOREN: Frédéric Hofer | Hasan Balci | Simon Gemetti | Marcel Spahr
REPOSITORY: https://github.com/simongemetti/Gruppe-Covid-App

SWISS COVID CERT APP, ARCHITEKTURDOKUMENTATION (arc42)

Kompakte, bewertungsorientierte Dokumentation für Unterricht und Präsentation

VERSION: 1.1

DATUM: 08.11.2025

AUTOREN: Frédéric Hofer | Hasan Balci | Simon Gemetti | Marcel Spahr

REPOSITORY: https://github.com/simongemetti/Gruppe-Covid-App

INHALTSVERZEICHNIS

1 EINFÜHRUNG UND ZIELE: Worum geht es ?

1.1 Kurzbeschreibung der Fachanwendung: Swiss Covid Cert App in einem Satz

Die Swiss Covid Cert Wallet App speichert signierte Covid-Zertifikate lokal auf dem Smartphone. Die App zeigt Zertifikate bei Bedarf offline an und prüft deren Gültigkeit anhand digitaler Signaturen und einer vertrauenswürdigen Trustliste, die regelmässig vom FOITT/BAG-Backend bereitgestellt wird.

1.2 Motivation und Nutzen: Warum dieses System sinnvoll ist

Die App bietet einen einfachen, digitalen Nachweis des Impf-, Test- oder Genesungsstatus. Sie verzichtet vollständig auf zentrale Datenspeicherung und erfüllt damit hohe Anforderungen an den Datenschutz. Die App ist technisch kompatibel mit dem EU Digital Covid Certificate (DCC) und kann deshalb zuverlässig an Einlässen, Veranstaltungen und Grenzen genutzt werden.

1.3 Stakeholder und Zielgruppen: Wer profitiert

- **Nutzerinnen und Nutzer**, welche Zertifikate importieren, anzeigen und verwalten.
- **Prüfende Stellen**, die mit der separaten Covid Certificate Check App Zertifikate prüfen.
- **Behörden (BAG / FOITT)**, welche Trustlisten, Schlüssel und zentrale Backend-Komponenten betreiben.
- **App-Store-Plattformen**, die die mobilen Apps bereitstellen und aktualisieren.

1.4 Top-Qualitätsziele: Die drei wichtigsten Ziele

- **Sicherheit und Datenschutz:** Zuverlässige Signaturprüfung, minimale Datenweitergabe, kein Tracking.
- **Verfügbarkeit und Offline-Fähigkeit:** Die App funktioniert auch ohne Internetverbindung.
- **Performance und Benutzerfreundlichkeit:** Ein QR-Scan dauert im Median weniger als 0.5 Sekunden und die Bedienung bleibt intuitiv und klar.

1.5 Randbedingungen und Annahmen: Rahmen, Standards, Scope

- **Standards:** EU Digital Covid Certificate (DCC, CBOR/COSE), QR-Codes, TLS 1.2 oder höher.
- **Plattformen:** iOS und Android, Nutzung der OS-eigenen Secure-Storage-Mechanismen sowie Kamera-Zugriff.
- **Datenmodell:** Zertifikate bleiben lokal auf dem Gerät und werden nicht an Server übertragen.
- **Annahmen:** Die Dokumentation beschreibt ein Referenzmodell für Lernzwecke; produktive Systeme können abweichen.

1.6 Technische und organisatorische Rahmenbedingungen

Die Architektur der Swiss Covid Cert Wallet App basiert auf einer klaren Trennung zwischen lokalen und zentralen Komponenten. Die Wallet App läuft vollständig lokal auf dem Gerät. Das Backend wird nur genutzt, um die Trustliste abzurufen. Die Kommunikation zwischen App und Backend erfolgt ausschliesslich verschlüsselt und signiert. Das System erfüllt das Prinzip „Privacy by Design“ und die Vorgaben des schweizerischen Datenschutzgesetzes (DSG) sowie der DSGVO.

1.7 Ziel und Nutzen dieser Architekturdokumentation

Diese Dokumentation beschreibt die Softwarearchitektur der Swiss Covid Cert Wallet App strukturiert und nachvollziehbar. Sie dient als Grundlage für technische Entscheidungen, Sicherheitsbetrachtungen und Weiterentwicklungen. Die Dokumentation folgt dem arc42-Standard, wodurch sowohl technische als auch fachliche Stakeholder (BAG, FOITT, Entwicklerinnen, Architektinnen, Tester) die Architektur schnell erfassen können.

2 KONTEXT UND ABGRENZUNG

2.1 Fachlicher Kontext: Systemgrenze und Beteiligte

- Das Kontextdiagramm bildet das Systemumfeld der Swiss Covid Cert Wallet App ab. Zum Gesamtsystem gehören:
- Swiss Covid Cert Wallet App
- Covid Certificate Check App
- Ausstellungsanwendungen (z. B. Arztpraxen, Apotheken, Labore, Behördenportale)
- FOITT/BAG Backend (Trustlisten, PKI)
- EU DCC Gateway (internationaler Schlüssel- und Trustlistaustausch)

Akteure:

- **Nutzer/in:** Importiert, zeigt und verwaltet Zertifikate.
- **Ausstellende Stelle:** Erfasst Zertifikatsdaten und löst die Ausstellung eines Zertifikats aus.
- **Prüfende Stelle:** Prüft Zertifikate mit der Check App.
- **Betreiber/Entwicklung (BAG/FOITT):** Betreibt die Backend-Dienste, stellt Trustlisten bereit und definiert Sicherheitsvorgaben.

Umsysteme:

- **App Stores:** Verteilen die Wallet App und die Check App.
- **Ausstellungsanwendungen:** Senden Zertifikatsanträge und empfangen signierte Zertifikate.
- **EU DCC Gateway:** Synchronisiert Vertrauensanker und Konfigurationen.
- **Support/Helpdesk:** Unterstützt bei technischen Problemen.

2.2 Informationsflüsse

- **Nutzer/in → Wallet App:** Zertifikate importieren, anzeigen, verwalten
- **Ausstellende Stelle → Backend:** Zertifikatsantrag senden / signiertes Zertifikat empfangen
- **Prüfende Stelle → Check App:** QR-Code scannen / Gültigkeit anzeigen
- **App Stores → Smartphones:** App-Download und Updates
- **FOITT/BAG Backend → Geräte:** Trustliste herunterladen
- **FOITT/BAG Backend ↔ EU DCC Gateway:** Austausch von Trustlisten und öffentlichen Schlüsseln
- **Support ↔ System:** Störungsmeldungen, Rückmeldungen

2.3 Diagramm: Kontextdiagramm

Das Kontextdiagramm (Abbildung 1) zeigt das Systemumfeld und die relevanten Akteure.

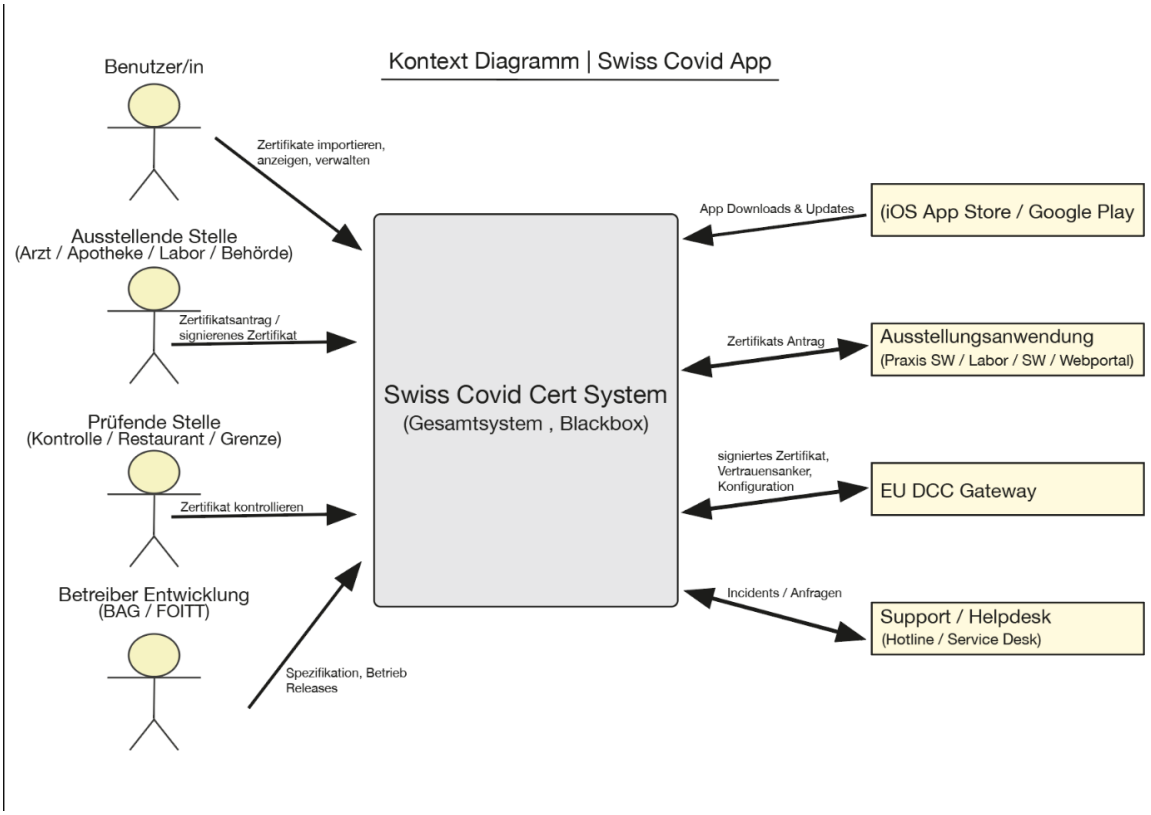


Abbildung 1: Kontext Diagramm

2.4 Erläuterung zum Kontextdiagramm

Das Kontextdiagramm zeigt alle relevanten Akteure, Umsysteme und Informationsflüsse. Technische Details der Implementierung werden bewusst weggelassen.

2.5 Konsistenz zum Systemkontext

Die Begriffe und Akteure werden in den folgenden Kapiteln vollständig konsistent weitergeführt.

3 ANWENDUNGSFÄLLE: Use-Case-Diagramm

3.1 Use-Case-Übersicht: Akteure und Fälle

- **Nutzer/in**
- **Vertretende Person (z. B. Elternteil)**
- **Prüf App (Check App)**
- **FOITT/BAG Trustlist Service**

3.2 Diagramm: Anwendungsfalldiagramm

Die Akteure der Wallet App sind:

Nutzer/in

Vertretende Person

Covid Certificate Check App (indirektes System)

FOITT/BAG Trustlist Service

Die Use Cases der Wallet App umfassen:

UC1 Zertifikat importieren

UC2 Zertifikat anzeigen

UC3 Zertifikat verwalten

UC4 Zertifikat vorzeigen

UC5 Gültigkeit lokal prüfen

UC6 Transfer-Code erzeugen / einlösen

UC7 Zertifikat exportieren / teilen

UC8 Trustliste aktualisieren

UC9 App schützen

UC10 Hilfe / FAQ anzeigen

Abbildung 2 zeigt das vollständige Use-Case-Diagramm der Wallet App.

3.3 Diagramm: Anwendungsfalldiagramm 01 (Covid Cert App)

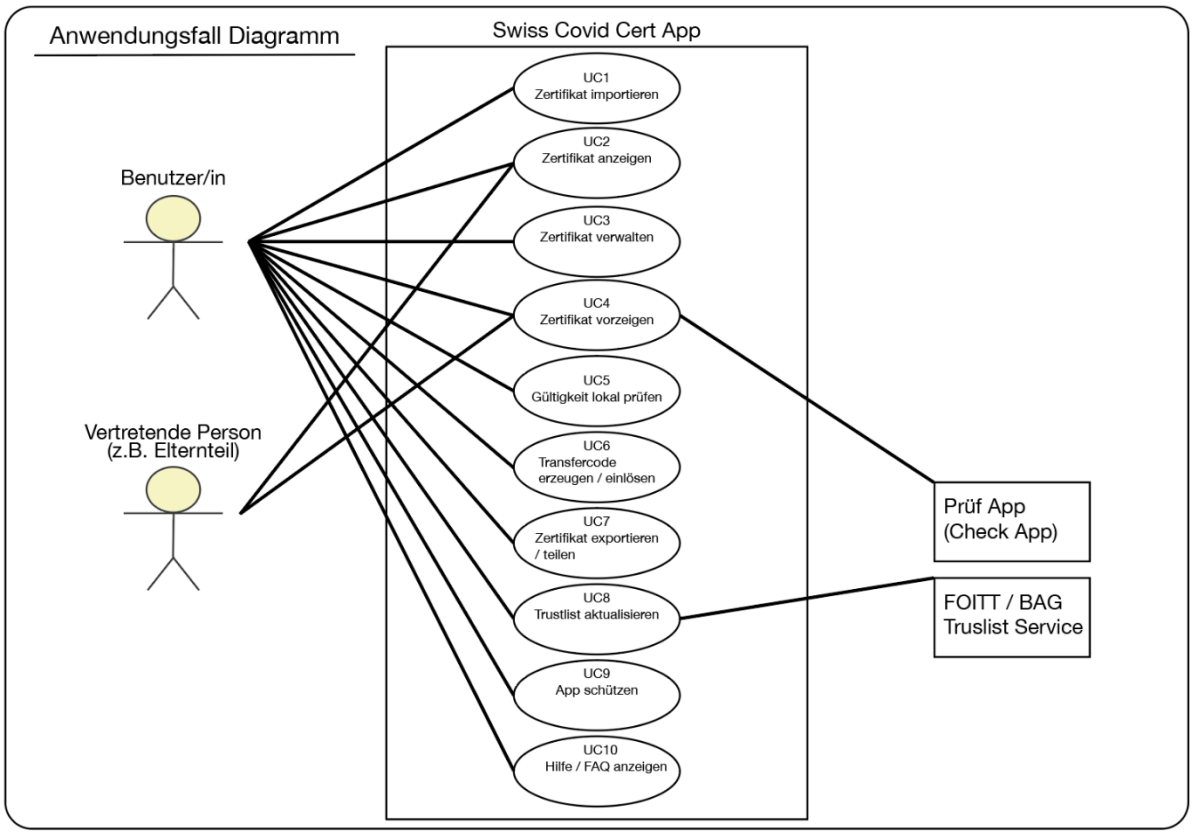


Abbildung 2: Anwendungsfall Diagramm

3.4 Kurzbeschreibungen pro Use Case: Ziel, Ablauf, Bedingungen

UC1 – Zertifikat importieren

Der Nutzer importiert ein Covid-Zertifikat über einen QR-Code oder eine Datei. Die App liest das Zertifikat ein und prüft anschliessend automatisch die Gültigkeit über UC5. Bei erfolgreicher Prüfung wird das Zertifikat lokal gespeichert und erscheint in der Übersicht.

UC2 – Zertifikat anzeigen

Die App zeigt ein ausgewähltes Zertifikat übersichtlich an. Die Anzeige kann von der prüfenden Stelle gescannt werden. Eine vertretende Person kann ebenfalls Zertifikate anzeigen, falls sie diese Verantwortung übernimmt.

UC3 – Zertifikat verwalten (benennen, löschen, ordnen)

Nutzerinnen und Nutzer können Zertifikate umbenennen, löschen oder in der Reihenfolge anpassen. Die Änderungen werden lokal gespeichert.

UC4 – Zertifikat vorzeigen

Das Zertifikat wird gross und gut lesbar angezeigt, damit eine prüfende Stelle den Code mit der Check App scannen kann. Die App zeigt bewusst keine zusätzlichen Personendaten an, um den Datenschutz zu gewährleisten.

UC5 – Gültigkeit lokal prüfen

Die App prüft die Signatur und die zeitliche Gültigkeit eines Zertifikats anhand der heruntergeladenen Trustliste. Die Prüfung erfolgt vollständig offline.

UC6 – Transfer Code erzeugen / einlösen

Der Nutzer kann Zertifikate zwischen Geräten übertragen, ohne diese erneut importieren zu müssen. Dafür wird ein temporärer Transfer-Code erzeugt und auf dem Zielgerät wieder eingelöst.

UC7 – Zertifikat exportieren / teilen

Zertifikate können als PDF oder Bild exportiert und über andere Apps geteilt werden.

UC8 – Trustlist aktualisieren

Die App lädt periodisch oder manuell eine signierte Trustliste vom FOITT/BAG Backend herunter.

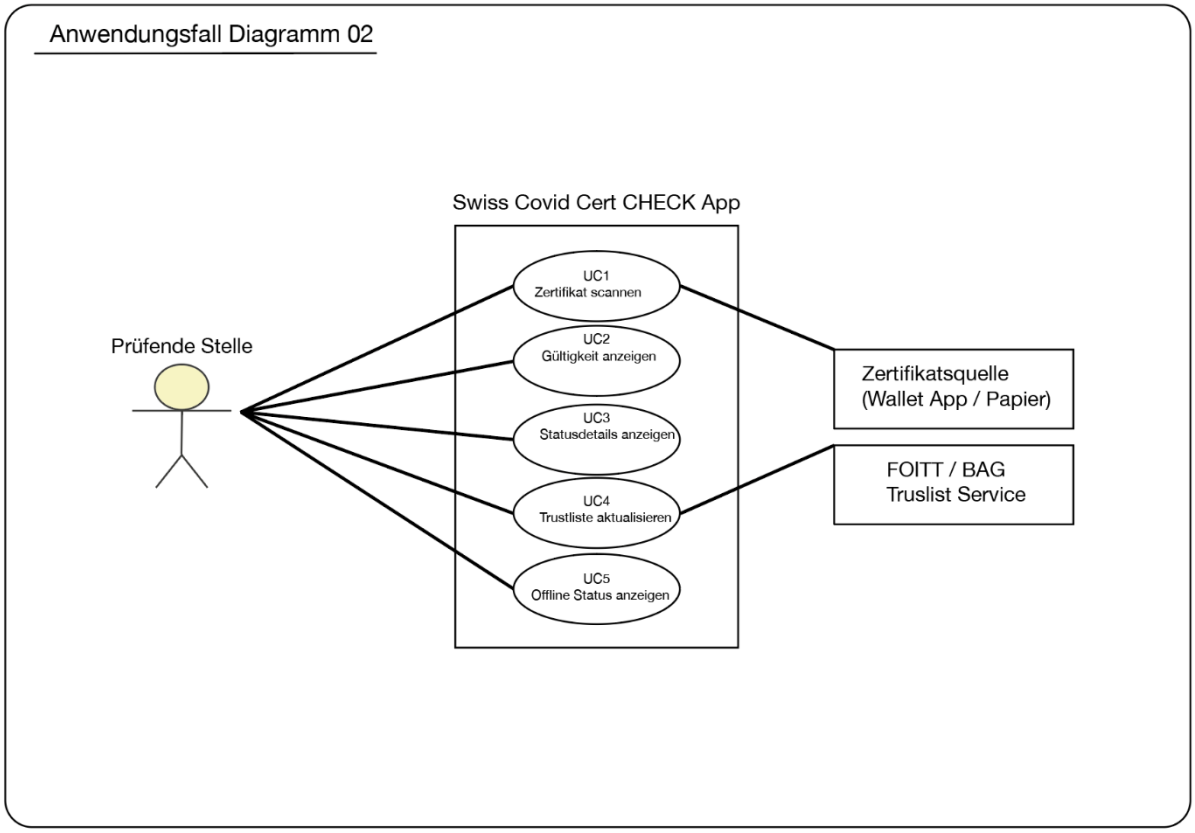
UC9 – App schützen

Die App kann mit Face ID, Touch ID oder einem App-Passcode geschützt werden.

UC10 – Hilfe / FAQ anzeigen

Die App zeigt eine kurze, übersichtliche FAQ mit Hinweisen zur Nutzung.

3.5 Diagramm: Anwendungsfalldiagramm 02 (Check App)



Die Covid Certificate Check App wird von prüfenden Stellen eingesetzt, um den QR-Code eines Covid-Zertifikats zu scannen und die Gültigkeit lokal zu prüfen. Die App arbeitet vollständig offline und nutzt ausschliesslich die lokal gespeicherte Trustliste. Das Anwendungsfalldiagramm zeigt die zentralen Abläufe und beteiligten Akteure.

Akteure der Check App
Prüfende Stelle
(z. B. Sicherheitspersonal, Restaurant, Veranstalter, Behörden)
Zertifikatsquelle
(Swiss Covid Cert Wallet App oder ein gedrucktes Zertifikat)
FOITT / BAG Trustlist Service

Use Cases der Check App

UC1: Zertifikat scannen
UC2: Gültigkeit anzeigen
UC3: Statusdetails anzeigen
UC4: Trustliste aktualisieren
UC5: Offline-Status anzeigen

Das Diagramm zeigt, dass nach dem Scanvorgang (UC1) automatisch UC2 ‘Gültigkeit anzeigen’ ausgeführt wird (<>). Zusätzlich kann UC2 bei Bedarf UC3 ‘Statusdetails anzeigen’ auslösen (<>)

3.6 Beschreibung der Use Cases (Check App)

UC1 – Zertifikat scannen
Ziel:
Die App liest den QR-Code eines Zertifikats ein, um anschliessend die Gültigkeit zu prüfen.

Akteure:
Prüfende Stelle, Zertifikatsquelle (Wallet App oder Papier).

Voraussetzungen:
Die App ist gestartet; der QR-Code ist sichtbar.

Nachbedingungen:
Die Zertifikatsdaten wurden erfolgreich eingelesen und stehen für UC2 zur Verfügung.

Hauptablauf:
Die prüfende Stelle öffnet die Check App.
Die Kamera wird aktiviert.
Der QR-Code wird gescannt.
Die App dekodiert die Zertifikatsdaten.
Die Daten werden an UC2 „Gültigkeit anzeigen“ übergeben.

UC2 – Gültigkeit anzeigen

Ziel:
Die App zeigt an, ob das eingelesene Zertifikat gültig, abgelaufen oder ungültig ist.

Akteure:
Prüfende Stelle.

Voraussetzungen:
UC1 wurde erfolgreich ausgeführt und die Zertifikatsdaten liegen vor.

Nachbedingungen:
Der Status des Zertifikats wird angezeigt.

Hauptablauf:
UC1 liefert die Zertifikatsdaten.
Die App prüft die Signatur mit der lokalen Trustliste.
Die App prüft zeitliche Bedingungen (z. B. Ablaufdatum).
Die Gültigkeit wird visuell angezeigt (z. B. grün/rot).
Optional kann UC3 aufgerufen werden.

UC3 – Statusdetails anzeigen

Ziel:
Zusätzliche Informationen zum Zertifikat und Prüfergebnis anzeigen.

Akteure:
Prüfende Stelle.

Voraussetzungen:
UC2 wurde ausgeführt.

Nachbedingungen:
Detaillierte Informationen werden angezeigt, ohne die Gültigkeit zu verändern.

Hauptablauf:
Die prüfende Stelle wählt „Details anzeigen“.
Die App zeigt zusätzliche Informationen, z. B. Zertifikatsart, Zeiträume oder technische Hinweise.
Die prüfende Stelle kehrt zurück zur Hauptansicht.

UC4 – Trustliste aktualisieren

Ziel:
Die lokale Trustliste wird manuell oder periodisch aktualisiert.

Akteure:
Prüfende Stelle, FOITT/BAG Trustlist Service (indirekt).

Voraussetzungen:
Internetverbindung vorhanden.

Nachbedingungen:
Eine aktualisierte, signierte Trustliste ist lokal gespeichert.

Hauptablauf:
Die prüfende Stelle startet die Aktualisierung oder die App führt diese im Hintergrund aus.
Die App lädt die signierte Trustliste vom Backend.
Die Signatur der Liste wird geprüft.
Die neue Liste wird aktiviert.

UC5– Offline Status anzeigen

Ziel:
Die App zeigt transparent an, ob die Prüfung vollständig oder nur eingeschränkt möglich ist.

Akteure:

Prüfende Stelle.

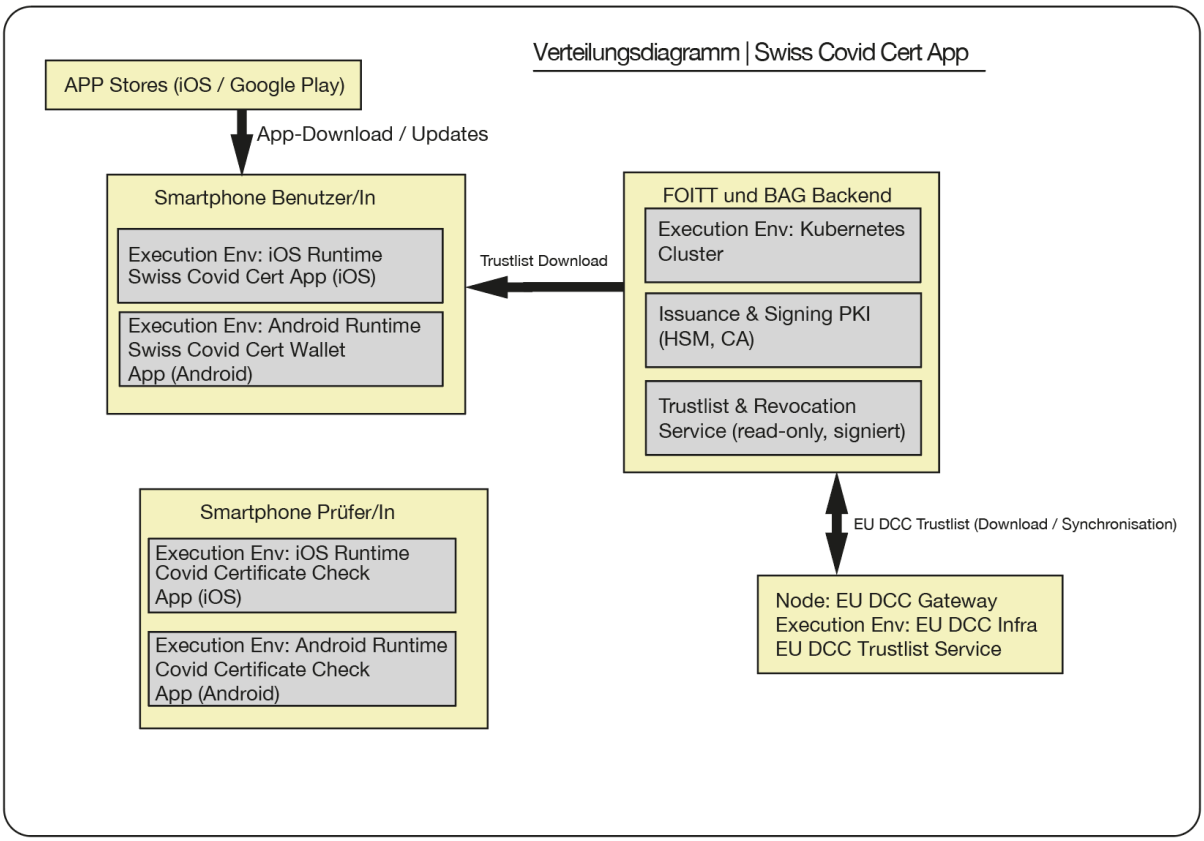
Voraussetzungen:
Die App ist gestartet.

Nachbedingungen:
Die prüfende Stelle versteht, ob die Trustliste aktuell ist oder nicht.

Hauptablauf:
Beim Start prüft die App, ob die Trustliste aktuell ist.
Die App zeigt an, ob der Prüfmodus „online“ oder „offline / Trustliste veraltet“ ist.
Die prüfende Stelle kann bei Bedarf UC4 auslösen.

4 VERTEILUNGSSICHT (arc42-7): Deployment und technische Zuordnung

Dieses Kapitel beschreibt, wie die Swiss Covid Cert Lösung technisch verteilt ist. Es zeigt, auf welchen Geräten und in welchen Umgebungen die einzelnen Komponenten laufen, und wie diese Geräte miteinander kommunizieren. Das Deploymentdiagramm stellt die beteiligten Knoten (Nodes), ihre Ausführungsumgebungen (Runtimes) und die darauf installierten Softwarekomponenten dar.



4.1 Übersicht der Knoten und Komponenten:

Die Swiss Covid Cert Lösung besteht aus mehreren klar abgegrenzten technischen Knoten:

- Smartphones der Nutzerinnen und Nutzer (mit der Swiss Covid Cert Wallet App)
- Smartphones der prüfenden Stellen (mit der Covid Certificate Check App)
- Den App Stores von Apple und Google
- Dem FOITT/BAG Backend, das Trustlisten und Schlüssel bereitstellt
- Dem EU DCC Gateway für den internationalen Austausch von Vertrauensankern

Alle mobilen Apps laufen vollständig lokal auf den Geräten. Für die Trustlisten und technischen Konfigurationsdaten wird das Backend genutzt. Der Aufbau ist bewusst schlank und darauf ausgelegt, auch bei fehlender Internetverbindung zuverlässig zu funktionieren.

4.2 Knoten und Ausführungsumgebung

4.2.1 APP Stores (iOS / Google Play)

Die App Stores sind der Ausgangspunkt für die Verteilung der mobilen Anwendungen. Sie betreiben eine eigene Serverinfrastruktur, über welche:
die Swiss Covid Cert Wallet App
und die Covid Certificate Check App

an die Endgeräte ausgeliefert und aktualisiert werden.
Es findet kein fachlicher Datenaustausch statt, sondern ausschliesslich die Bereitstellung der App-Binärpakete.

4.2.2 Smartphone Nutzer/in

Auf dem Gerät der Nutzerinnen und Nutzer laufen die beiden Varianten der Wallet App innerhalb der jeweiligen Ausführungsumgebung:

- **iOS Runtime:** Swiss Covid Cert Wallet App (iOS)
- **Android Runtime:** Swiss Covid Cert Wallet App (Android)

Die Wallet App speichert Zertifikate lokal auf dem Gerät und führt die gesamte Signatur- und Gültigkeitsprüfung direkt auf dem Smartphone aus. Für die Trustlisten wird periodisch oder manuell eine Verbindung zum FOITT/BAG Backend aufgebaut.

4.2.3 Smartphone Prüfer/in

Prüfende Stellen nutzen ein separates Gerät mit der Covid Certificate Check App. Die App läuft innerhalb folgender Ausführungsumgebungen:
iOS Runtime: Covid Certificate Check App (iOS)
Android Runtime: Covid Certificate Check App (Android)

Die Check App funktioniert vollständig offline und prüft QR-Codes anhand der lokal gespeicherten Trustliste. Sie stellt keine direkte Verbindung zum Backend her.

4.2.4 FOITT / BAG Backend

Das Backend des FOITT/BAG bildet die zentrale technische Infrastruktur. Es läuft in einem Kubernetes-Cluster und stellt mehrere Backend-Komponenten bereit:
Issuance & Signing PKI: Verantwortlich für die signierte Ausstellung von Zertifikaten und den sicheren Umgang mit privaten Schlüsseln (HSM, CA).
Trustlist & Revocation Service: Liefert signierte Trustlisten und Sperrlisten an mobile Geräte aus.

Die Backend-Komponenten sind hochverfügbar und sicherheitsgehärtet. Sie enthalten keinerlei persönliche Zertifikatsdaten. Die PKI-Schlüssel bilden das Sicherheitsfundament des gesamten Systems.

4.2.5 EU DCC Gateway

Der EU DCC Gateway-Knoten ermöglicht den Austausch von Vertrauensankern mit der EU und weiteren teilnehmenden Staaten. Auf diesem Node laufen:
Execution Environment: EU DCC Trustlist Infrastruktur
EU DCC Trustlist Service: verarbeitet und synchronisiert Trustlisten und öffentliche Schlüssel

Damit wird sichergestellt, dass Zertifikate aus der Schweiz auch im Ausland gültig geprüft werden können – und umgekehrt.

4.3 Kommunikationsbeziehungen

4.3.1 APP Stores → Smartphones
App-Download und Updates
Keine fachlichen Daten
Reiner Distributionskanal

4.3.2 FOITT/BAG Backend → Smartphones
Trustlist Download über HTTPS (signiert)
Wird von der Wallet App direkt genutzt
Die Check App erhält die aktualisierte Trustliste über den Betriebssystem-Mechanismus

4.3.3 FOITT/BAG Backend ↔ EU DCC Gateway
Austausch der Trustlisten, öffentlichen Schlüssel und Konfigurationsdaten
Grundlage für internationale Interoperabilität
Die Daten werden kryptografisch gesichert und validiert

Keine direkte Kommunikation:
Zwischen Wallet-App und Check-App (kein technischer Kanal, QR-Code ist kein Deployment-Flow)
Zwischen Check-App und Backend (Check-App ist offline-fähig)
Zwischen App Stores und Backend (getrennte Infrastruktur)

Diese klare Trennung entspricht genau der Datenschutzphilosophie von Swiss Covid Cert:
So wenig zentrale Daten wie möglich – so viel lokale Verarbeitung wie nötig.

4.4 Verteilungsdiagramm

Das Verteilungsdiagramm in Abbildung 4 zeigt alle Knoten, deren Ausführungsumgebungen und die darin installierten Komponenten.

Es bildet die technische Struktur der gesamten Swiss Covid Cert Lösung vollständig ab.
Das Diagramm folgt der UML Deployment Notation (Variante A), bei der:
Nodes als Kästen dargestellt werden
Execution Environments innerhalb der Nodes liegen
Artefakte (Apps, Komponenten) innerhalb der Runtimes liegen
Kommunikationsbeziehungen als gerichtete Pfeile dargestellt werden

Die Darstellung ist bewusst klar gehalten, damit die Architektur auch für Personen ohne technischen Hintergrund nachvollziehbar bleibt.

5 QUALITÄTSANFORDERUNGEN

Die Swiss Covid Cert Lösung stellt hohe Anforderungen an Sicherheit, Datenschutz und Verfügbarkeit. Die folgenden Qualitätsanforderungen beschreiben die zentralen nicht-funktionalen Eigenschaften des Systems. Sie sind massgebend für die technische Umsetzung, die Auswahl der Komponenten sowie die Architekturentscheidungen, die in dieser Dokumentation dargestellt wurden.

5.1 Qualitätsziele

Beschreibung:
Die Wallet App speichert alle Zertifikatsdaten lokal auf dem Gerät. Sie überträgt keine persönlichen Informationen an das Backend. Die Gültigkeitsprüfung erfolgt ausschliesslich anhand der Signatur des Zertifikats und einer signierten Trustliste. Dadurch bleibt der Datenschutz auch bei intensiver Nutzung jederzeit gewährleistet.

Ziel:
Sensible Daten sollen zu keinem Zeitpunkt auf Servern landen. Die Signaturprüfung muss zuverlässig erkennen, ob ein Zertifikat echt, gültig oder manipuliert wurde.

Szenario:
Eine Nutzerin öffnet ihr Zertifikat und zeigt es an einer Veranstaltung vor. Dabei findet keinerlei Datenübermittlung statt. Die prüfende Stelle sieht ausschliesslich die Informationen, die im QR-Code codiert sind. Das Backend erkennt die Nutzung nicht, und es wird kein Zugriffsprotokoll erzeugt.

Bewertungskriterium:
Die Architektur muss garantieren, dass keine Personendaten das Gerät verlassen und dass die Signaturprüfung fälschungssicher funktioniert.

5.2 Qualitätsszenario 2: Verfügbarkeit und Offline-Fähigkeiten

Beschreibung:
Eine der wichtigsten Anforderungen ist die Funktionsfähigkeit ohne Internetverbindung. Sowohl die Wallet App als auch die Check App müssen offline Zertifikate prüfen können. Der Grund dafür ist die Nutzung an Orten, an denen keine stabile Verbindung vorhanden ist (z. B. Konzerte, Stadien, Grenzgebiete).

Ziel:

Die Gültigkeitsprüfung soll in jeder Situation funktionieren, unabhängig von der Netzabdeckung.

Szenario:
Eine prüfende Stelle scannt ein Zertifikat an einem belebten Eingang, wo das Mobilfunknetz stark ausgelastet ist. Die Check App prüft die Signatur des Zertifikats mit der lokal gespeicherten Trustliste und zeigt den Status sofort an.

Bewertungskriterium:
Die Gültigkeitsprüfung muss auch ohne Internet in der gewohnt hohen Qualität funktionieren. Die Trustliste muss regelmässig aktualisiert werden können, ohne die Offline-Fähigkeit zu beeinträchtigen.

5.3 Qualitätsszenario 3: Performance und Benutzerfreundlichkeit

Beschreibung:
Die App muss schnell reagieren und eine klare, verständliche Benutzeroberfläche bieten. Da Zertifikatsprüfungen oft unter Zeitdruck stattfinden (z. B. beim Einlass), sind kurze Antwortzeiten entscheidend.

Ziel:
Die Bedienung soll intuitiv sein und nicht mehr als wenige Sekunden beanspruchen.

Szenario:
Ein Nutzer importiert ein Zertifikat. Die App liest den QR-Code, führt die Signaturprüfung durch und zeigt das Zertifikat innerhalb von unter einer Sekunde vollständig an. Bei der Check App soll der Status nach dem Scan ebenfalls nahezu sofort erscheinen.

Bewertungskriterium:
Der Zeitraum zwischen Scan und Anzeige darf den Medianwert von 0.5 Sekunden nicht überschreiten. Die Benutzeroberfläche muss klar strukturiert und ohne unnötige Ablenkungen gestaltet sein.

5.4 Zusammenfassung der Qualitätsanforderungen

Die drei definierten Qualitätsszenarien bilden die wichtigsten nicht-funktionalen Anforderungen der Swiss Covid Cert Lösung ab. Sie zeigen klar auf, wie Sicherheit, Datenschutz, Offline-Fähigkeit, Performance und Benutzerfreundlichkeit zusammenspielen.

- Die Architektur schützt die Privatsphäre der Nutzerinnen und Nutzer.
- Die Lösung funktioniert zuverlässig auch ohne Internet.
- Die Apps reagieren schnell und sind einfach verständlich aufgebaut.

Dadurch erfüllt die Swiss Covid Cert App sowohl technische Anforderungen als auch die Erwartungen der Anwenderinnen und Anwender in der Praxis.

6 GLOSSAR:

Dieses Glossar definiert die wichtigsten Begriffe, die im Zusammenhang mit der Swiss Covid Cert Lösung verwendet werden. Die Begriffe sind bewusst kurz und verständlich erklärt, damit sowohl technische als auch fachliche Leserinnen und Leser die Inhalte ohne Hintergrundwissen nachvollziehen können.

App Stores
Infrastruktur von Apple (App Store) und Google (Play Store), über welche die Swiss Covid Cert Wallet App und die Covid Certificate Check App heruntergeladen und aktualisiert werden.

Ausstellungsanwendung
Software einer Arztpraxis, eines Labors oder einer Behörde, mit der Zertifikatsdaten erfasst und Zertifikatsanträge erstellt werden. Diese Anwendungen senden die Daten an das FOITT/BAG Backend und erhalten ein signiertes Zertifikat zurück.

BAG
Bundesamt für Gesundheit. Zuständig für regulatorische Vorgaben, Spezifikationen, Sicherheitsanforderungen und den fachlichen Betrieb des Swiss Covid Cert Systems.

Check App (Covid Certificate Check App)
Mobile App für prüfende Stellen. Sie scannt den QR-Code eines Zertifikats und zeigt dessen Gültigkeit an. Die App funktioniert vollständig offline und nutzt die lokal gespeicherte Trustliste.

DCC (EU Digital Covid Certificate)
Europäischer Standard für Covid-Zertifikate. Er definiert Datenformate, Signaturstrukturen und Prüfmechanismen, damit Zertifikate international kompatibel bleiben.

FOITT
Bundesamt für Informatik und Telekommunikation. Verantwortlich für Betrieb, Sicherheit und Bereitstellung der Backend-Komponenten wie Trustlisten und PKI.

Gültigkeitsprüfung
Technischer Prozess, bei dem die App die Signatur des Zertifikats prüft und den zeitlichen Gültigkeitszeitraum validiert. Diese Prüfung erfolgt vollständig lokal in der Wallet App oder der Check App.

PKI (Public Key Infrastructure)
Kryptografisches System zur Verwaltung von Schlüsseln und Zertifikaten. Im Swiss Covid Cert System stellt die PKI sicher, dass Zertifikate korrekt signiert und fälschungssicher sind.

Smartphone Nutzer/in

Endgerät, auf welchem die Swiss Covid Cert Wallet App läuft. Die App speichert Zertifikate lokal und zeigt sie bei Bedarf offline an.

Smartphone Prüfer/in
Endgerät, auf welchem die Covid Certificate Check App installiert ist. Es wird verwendet, um Zertifikate zu prüfen, ohne dass eine Online-Verbindung benötigt wird.

Trustliste
Liste der öffentlichen Schlüssel, die zur Signaturprüfung genutzt werden. Die Trustliste wird regelmässig vom FOITT/BAG Backend heruntergeladen und lokal gespeichert.

Wallet App (Swiss Covid Cert Wallet App)
Mobile App, welche Zertifikate importiert, verwaltet und anzeigt. Die App führt Gültigkeitsprüfungen offline durch und speichert alle Zertifikatsdaten ausschliesslich lokal.