

# Die deutsche Corona Warn-App.

Ein prägnanter Überblick über die  
Softwarearchitektur der  
Gesamtlösung – Apps und Backend.



STAND: APRIL 2021

**embarc**   
Software Consulting GmbH

## Über diesen Foliensatz ...

Die Inhalte dieses Überblicks entstanden im Rahmen eines Architektur-Reviews  
2020/2021. Gezeigt wurden sie erstmals in diesem Vortrag:



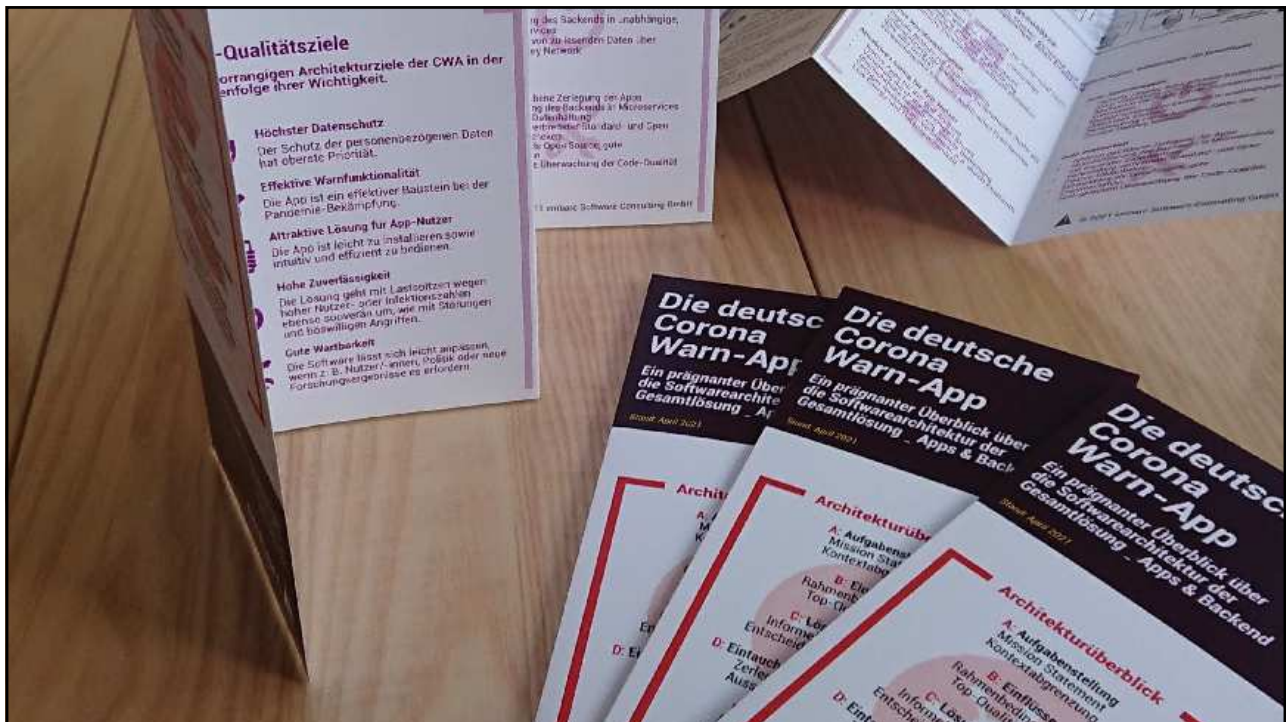
### So gehen Architektur-Reviews!

Die deutsche Corona-Warn-App unter der Lupe  
Sprecher: Stefan Zörner (embarc) und Falk Sippach (embarc)  
OOP-Konferenz 2021  
Mittwoch, 10. Februar 2021, 09:00 - 10:30 Uhr, online

Anschließend sind die Diagramme und Texte in einem verdichteten Flyer aufgegangen,  
der als Beispiel für prägnante Architekturüberblicke dient.

Der vorliegende Foliensatz zeigt die Inhalte in einem Format, das sich für  
Präsentationen eignet. Wir hoffen, er gibt Ihnen Orientierung, wenn Sie Eckpunkte Ihrer  
Softwarelösung Dritten – z.B. Neuen Teammitgliedern – vorstellen wollen.





## Architekturüberblick

- A: Aufgabenstellung**  
Mission Statement  
Kontextabgrenzung
- B: Einflüsse**  
Rahmenbedingungen  
Top-Qualitätsziele
- C: Lösungsstrategie**  
Informelles Überblicksbild  
Entscheidende Lösungsansätze
- D: Eintauchen in die Corona-Warn-App**  
Zerlegung auf oberster Ebene  
Ausschnitt Technologie-Stack
- E: Bewertung & Ausblick**  
Ausgewählte Kompromisse  
Nächste Schritte für die CWA  
Weitere Informationen



## Architekturüberblick

### A: Aufgabenstellung

Mission Statement  
Kontextabgrenzung

### B: Einflüsse

Rahmenbedingungen  
Top-Qualitätsziele

### C: Lösungsstrategie

Informelles Überblicksbild  
Entscheidende Lösungsansätze

### D: Eintauchen in die Corona-Warn-App

Zerlegung auf oberster Ebene  
Ausschnitt Technologie-Stack

### E: Bewertung & Ausblick

Ausgewählte Kompromisse  
Nächste Schritte für die CWA  
Weitere Informationen



## Mission Statement

### Was ist die Corona-Warn-App?

Die Corona-Warn-App (kurz CWA) hilft Infektionsketten des SARS-CoV-2 (COVID-19-Auslöser) in Deutschland nachzuverfolgen und zu unterbrechen.

Die App basiert auf Technologien mit einem dezentralisierten Ansatz und informiert Personen, wenn sie mit einer infizierten Person in Kontakt standen.

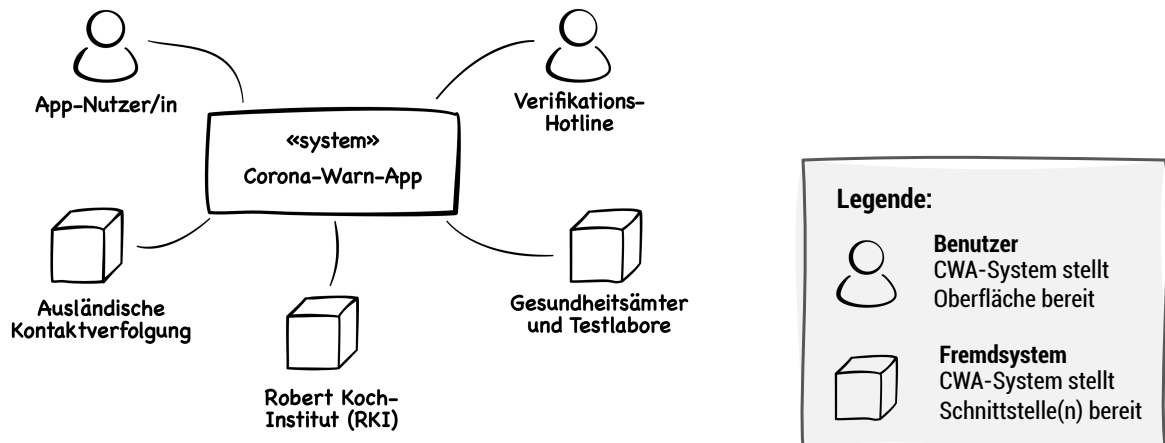
Transparenz ist von entscheidender Bedeutung, um die Bevölkerung zu schützen und die Akzeptanz zu erhöhen.

nach [www.coronawarn.app/de/](https://www.coronawarn.app/de/)



## Fachliche Kontextabgrenzung

Das CWA-Gesamtsystem im Zusammenspiel mit den wichtigsten Benutzern und Fremdsystemen.



## Fachliche Kontextabgrenzung, Akteure

Kurze Erläuterungen zu den Benutzern und Fremdsystemen:

Akteur	Beschreibung
App-Nutzer/in	Erhält Informationen über mögliche Begegnungen mit infizierten Personen und eigene Testergebnisse. Verifiziert eigene Testergebnisse und warnt so freiwillig andere.
Verifikations-Hotline	Unterstützt App-Nutzer/innen bei der Freischaltung positiver Testergebnisse ("teleTAN").
Gesundheitsämter und Testlabore	Liefern anonymisierte Testergebnisse an das System.
Robert Koch-Institut (RKI)	Stellt Inhalte ("Content") für die App zur Verfügung und bestimmt Parameter für die Messung der Kontakte ("Risiko-Ermittlung"). Empfängt Auswertungen, etwa aus der Datenspende.
Ausländische Kontaktverfolgungen	Austausch mit dezentralen Anwendungen anderer Länder zur grenzüberschreitenden Ermittlung von Kontakten.



## Architekturüberblick

### A: Aufgabenstellung

Mission Statement  
Kontextabgrenzung

### B: Einflüsse

Rahmenbedingungen  
Top-Qualitätsziele

### C: Lösungsstrategie

Informelles Überblicksbild  
Entscheidende Lösungsansätze

### D: Eintauchen in die Corona-Warn-App

Zerlegung auf oberster Ebene  
Ausschnitt Technologie-Stack

### E: Bewertung & Ausblick

Ausgewählte Kompromisse  
Nächste Schritte für die CWA  
Weitere Informationen



## Rahmenbedingungen CWA

Ausgewählte Maßgaben an Entwicklung und Betrieb sowie einige Informationen zum politischen Umfeld.

### Technische Vorgaben

- Entwicklung von nativen, mobilen Clients für Android- und iOS-Smartphones
- Verfolgen eines dezentralen Ansatzes für die Datenspeicherung
- Einsatz des Exposure Notification Framework von Google und Apple
- Betrieb der Backend-Komponenten in der Open Telekom Cloud



## Rahmenbedingungen CWA (Fortsetzung)

### Organisatorischer Rahmen und Umfeld

- Auftraggeber: Deutsche Bundesregierung
- Entwicklung und Betrieb durch ein Konsortium aus zwei Auftragnehmern (SAP und Deutsche Telekom)
- Start der Entwicklung 04/2020
- enger Zeitrahmen (Apps zum Download verfügbar ab 06/2020)
- hoher politischer Druck, viele Parteien involviert (Ministerien, Behörden, RKI ...)
- große Medienaufmerksamkeit
- gewisse Skepsis innerhalb der Bevölkerung



## Top-Qualitätsziele

Die vorrangigen Architekturziele der CWA in der Reihenfolge ihrer Wichtigkeit.

Ziel	Beschreibung
 <b>Höchster Datenschutz</b>	Der Schutz der personenbezogenen Daten hat oberste Priorität. <i>(Sicherheit)</i>
 <b>Effektive Warnfunktionalität</b>	Die App ist ein effektiver Baustein bei der Pandemie-Bekämpfung. <i>(Funktionale Eignung)</i>
 <b>Attraktive Lösung für App-Nutzer</b>	Die App ist leicht zu installieren sowie intuitiv und effizient zu bedienen. <i>(Benutzbarkeit)</i>
 <b>Hohe Zuverlässigkeit</b>	Die Lösung geht mit Lastspitzen wegen hoher Nutzer- oder Infektionszahlen ebenso souverän um, wie mit Störungen und böswilligen Angriffen. <i>(Zuverlässigkeit)</i>
 <b>Gute Wartbarkeit</b>	Die Software lässt sich leicht anpassen, wenn z. B. Nutzer/-innen, Politik oder neue Forschungsergebnisse es erfordern. <i>(Wartbarkeit/Erweiterbarkeit)</i>

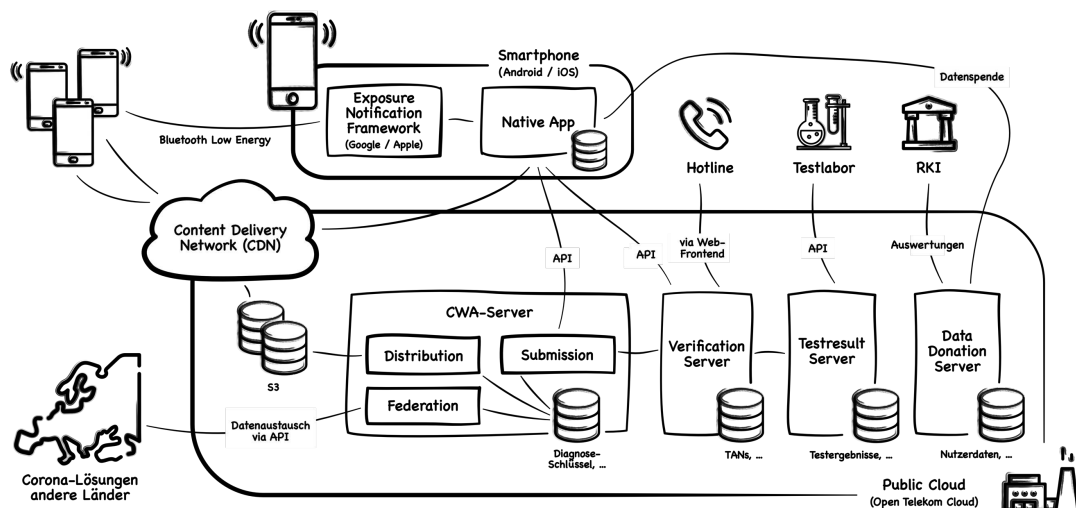


## Architekturüberblick

- A: Aufgabenstellung**  
Mission Statement  
Kontextabgrenzung
- B: Einflüsse**  
Rahmenbedingungen  
Top-Qualitätsziele
- C: Lösungsstrategie**  
Informelles Überblicksbild  
Entscheidende Lösungsansätze
- D: Eintauchen in die Corona-Warn-App**  
Zerlegung auf oberster Ebene  
Ausschnitt Technologie-Stack
- E: Bewertung & Ausblick**  
Ausgewählte Kompromisse  
Nächste Schritte für die CWA  
Weitere Informationen



## Informelles Überblicksbild



Quelle der Abbildung: S. Zörner, F. Sippach: „So gehen Architektur-Reviews! Entlang der Corona-Warn-App“, OOP 2021



## Entscheidende Lösungsansätze

Die aufgelisteten Prinzipien, Muster, Konzepte und Technologien adressieren die jeweiligen Top-Qualitätsziele und begünstigen deren Erreichung.

### Qualitätsziel: Höchster Datenschutz

- **Datensparsamkeit** (nur minimale, notwendige Informationen)
- **Dezentraler Ansatz**, Speicherung der Daten lokal beim App-Nutzer
- Verschlüsselung aller Bewegungsdaten
- Teilen von Daten nur nach Aufforderung
- Transparente Entwicklung (**Quelltexte** und Konzepte **einsehbar**)



## Entscheidende Lösungsansätze (2/3)

### Qualitätsziel: Effektive Warnfunktionalität

- **Digitale Abläufe** zur Risikowarnung
- Unterstützung der **gängigsten Smartphones** (mehr als 90% aller Geräte)
- Verwendung des Exposure Notification Frameworks

### Qualitätsziel: Attraktive Lösung für App-Nutzer

- **Native Apps** für iOS und Android
- Verteilung durch die jeweiligen Stores
- **Übersichtliche Gestaltung**, simple Bedienung
- **Geringer Ressourcen-Verbrauch**, u.a. durch Bluetooth Low Energy und Datensparsamkeit





## Entscheidende Lösungsansätze (3/3)

### Qualitätsziel: Hohe Zuverlässigkeit

- **Robuste Lösung**, Apps erfassen Begegnungen ohne Verbindung zum Backend
- Backend in der **Public Cloud**, Orchestrierung mit Kubernetes
- **Modularisierung** des Backends in unabhängige, skalierbare Services
- Bereitstellung von zu lesenden Daten über **Content Delivery Network**

### Qualitätsziel: Gute Wartbarkeit

- Fachlich getriebene Zerlegung der Apps
- **Modularisierung** des Backends in Microservices mit separater Datenhaltung
- Verwendung verbreiteter Standard- und Open Source-Bibliotheken
- Entwicklung als Open Source, **gute Dokumentation**
- Tool-gestützte Überwachung der Code-Qualität

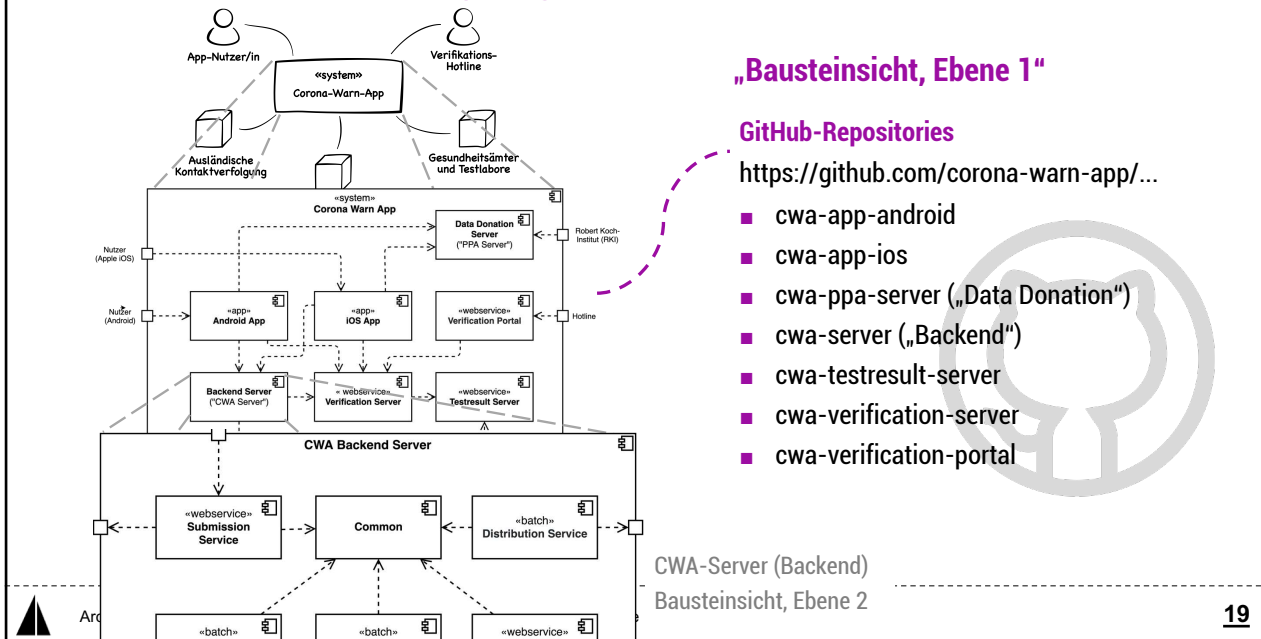


## Architekturüberblick

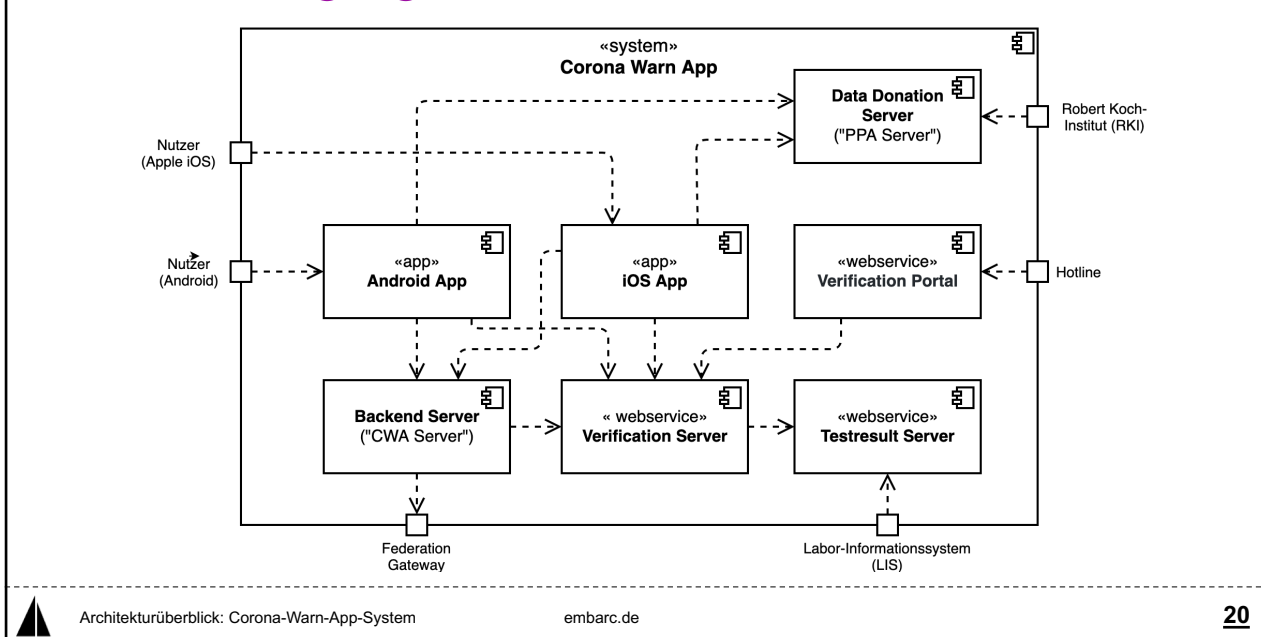
- A: Aufgabenstellung  
Mission Statement  
Kontextabgrenzung
- B: Einflüsse  
Rahmenbedingungen  
Top-Qualitätsziele
- C: Lösungsstrategie  
Informelles Überblicksbild  
Entscheidende Lösungsansätze
- D: Eintauchen in die Corona-Warn-App**  
Zerlegung auf oberster Ebene  
Ausschnitt Technologie-Stack
- E: Bewertung & Ausblick  
Ausgewählte Kompromisse  
Nächste Schritte für die CWA  
Weitere Informationen



## Tatsächliche Zerlegung im Quelltext



## Grobe Zerlegung (Bausteinsicht, Ebene 1)



## Grobe Zerlegung, Bausteine auf Ebene 1

Baustein	Wesentliche Aufgabe
iOS App	Native App für iPhones. Nutzt das GAEN-System von Google und Apple zur Kontaktermittlung. Ermittelt das Infektionsrisiko anhand von Diagnoseschlüsseln.
Android App	Native Android App, analog zur iOS App.
Backend Server (aka „CWA Server“)	Nimmt die Diagnoseschlüssel positiv getesteter Nutzer entgegen und teilt sie mit anderen Nutzern über ein CDN. Interagiert mit den Kontaktverfolgungen anderer Länder („Federation“).
Testresult Server	Empfängt und speichert die Testergebnisse von angeschlossenen Laboren.
Verification Server	Sichert ab, dass ein Nutzer zugestimmt hat, seinen positiven Test zu melden, und dass das Labor tatsächlich positiv getestet hat.
Verification Portal	Ermöglicht die Erzeugung von teleTANs im Verification Server über ein einfaches Browser-Frontend.
Data Donation Server (aka „PPA Server“)	Nimmt Nutzerdaten bei aktivierter Datenspende entgegen und speichert sie, ohne Rückschlüsse auf individuelle Personen zuzulassen. (PPA = Privacy Preserving Analytics)



## Ausschnitt Technologie-Stack (1/3)

Die CWA-Lösung verwendet diverse Programmiersprachen, Bibliotheken, Frameworks und Middleware.



### Client (Native Apps)

- iOS App programmiert in **Swift**
- Android App programmiert in **Kotlin**
- Persistenz mit **SQLite**
- Verteilung über **Google Play** (Android) und **App Store** (Apple iOS)



**Swift**



**Kotlin**



**SQLite**



## Ausschnitt Technologie-Stack (2/3)



### Server (Backend)

- Services programmiert in **Java** mit **Spring Boot**, Spring Cloud, Spring Data ...
- weitere Open Source Bibliotheken (u.a. Lombok, Guava, Liquibase, **Micrometer** ...)
- Kommunikation mit REST/**OpenAPI** und protobuf
- Persistenz mit **PostgreSQL**



## Ausschnitt Technologie-Stack (3/3)



### Infrastruktur

- Build mit **Maven**, **Gradle** und fastlane
- **Docker**, Docker Compose (zu Testzwecken), in Produktion auf **Kubernetes**
- S3 und Content Delivery Network (CDN)
- Betrieb in Public Cloud (**Open Telekom Cloud**)



## Architekturüberblick

- A: Aufgabenstellung**  
Mission Statement  
Kontextabgrenzung
- B: Einflüsse**  
Rahmenbedingungen  
Top-Qualitätsziele
- C: Lösungsstrategie**  
Informelles Überblicksbild  
Entscheidende Lösungsansätze
- D: Eintauchen in die Corona-Warn-App**  
Zerlegung auf oberster Ebene  
Ausschnitt Technologie-Stack
- E: Bewertung & Ausblick**  
Ausgewählte Kompromisse  
Nächste Schritte für die CWA  
Weitere Informationen



## Ausgewählte Kompromisse (1/2)

Der Entwurf der CWA geht bewusst Trade-offs ein und balanciert Qualitätsziele aus.

### Explizite Freigabe positiver Testergebnisse durch Nutzer/in erforderlich

- + erhöht Vertrauen in die Lösung
- reduziert effektive Warnfunktionalität



### Verteilte Anwendung auf dem Backend

- + gut für Datenschutz (Trennung der Daten)
- + verfügbar(er) im Falle von Teilausfällen
- schwieriger zu entwickeln und zu betreiben



## Ausgewählte Kompromisse (2/2)

### Ausliefern der Diagnoseschlüssel über CDN im Batch, Aktualisierung durch Apps in Intervallen

- + spart Ressourcen, vor allen an den Endgeräten
- + robust, erhöht Zuverlässigkeit
- Zeitverzögerung bei Risikoermittlung



### Vergleichsweise hohe Kopplung der Microservices (tw. synchrone Kommunikation, tw. geteilte Daten)

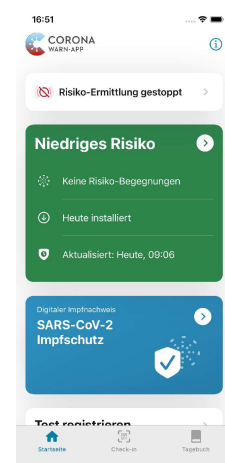
- + einfacher umzusetzen, schneller am Markt
- erschwert unabhängige Entwicklung
- reduziert oder behindert Zuverlässigkeit



## Nächste Schritte für die CWA

Auf Basis der Lösungsarchitektur wurden weitere Features angedacht, konzipiert oder auch bereits umgesetzt, z.B.

- lokales **Kontakttagbuch** (Nutzung optional)
- Anzeige ausgewählter **Kennzahlen** zum Infektionsgeschehen (Bereitstellung: RKI)
- **Eventregistrierung**, Einchecken mit QR-Code, Erkennen sogenannter Cluster
- Integration von **Schnelltestergebnissen**
- Anzeige eines **digitalen Impfnachweises**



## Weitere Informationen ...

... zur Corona-Warn-App

### Homepage des Open-Source-Projektes

- <https://www.coronawarn.app/de/>

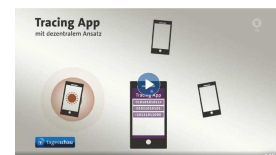
### Quelltexte und Dokumentation auf GitHub

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

### Beitrag Tagesschau vom 26.04.2020, Video (2 min)

„Bundesregierung setzt bei Corona-App auf dezentrale Datenspeicherung“

- <https://www.tagesschau.de/multimedia/video/video-693083.html>



## Weitere Informationen

..zu Architekturüberblicken

### Gesammeltes Material

Blog-Beiträge Vortragsvideos, weitere Beispiele im Netz

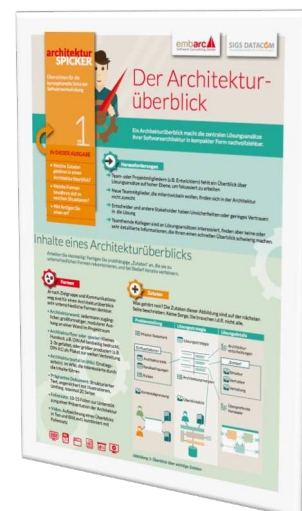
- <https://www.embarc.de/architektur-ueberblicke/>

### Kurzreferenz zum Thema

Architektur-Spicker #1: „Der Architekturüberblick“

4 Seiten, PDF zum Download

- <https://www.embarc.de/architektur-spicker/01-der-architekturueberblick/>



## Gibt es auch gedruckt!



Wir schicken Ihnen gerne ein gedrucktes Exemplar  
dieses Überblicks als Flyer im Treppenfalt zu!  
Einfach eine E-Mail senden an

[info@embarc.de](mailto:info@embarc.de)

mit Betreff „CWA-Flyer“ und Ihrer Postadresse im Text,  
dann geht das los ...



## Vielen Dank!

Wir freuen uns auf Ihre Fragen!



[sz@embarc.de](mailto:sz@embarc.de)



[@StefanZoerner](https://twitter.com/StefanZoerner)



➔ [xing.to/szr](https://xing.to/szr)



[fs@embarc.de](mailto:fs@embarc.de)



[@sippsack](https://twitter.com/sippsack)



➔ [xing.to/fsi](https://xing.to/fsi)

