

Assignment:

Quality Scenarios

**Student:** Jacob Müller

**Email:** Jacobmueller11@gmail.de

**Date of birth:** 10.02.1995

**Matriculation number:** 800913

**Academic institution:** Knowledge Foundation @ Reutlingen University

**Study program:** Master of Science Professional Software Engineering

Contents

[Introduction 2](#_Toc66691613)

[References 3](#_Toc66691614)

[Appendices 4](#_Toc66691615)

# Introduction

This assignment is created for the Software Architecture class of the Professional Software Engineering Masters Class of the Knowledge Foundation Reutlingen. The goal of this Assignment is to conduct.

The report will proceed as follows. First, a brief introduction to the Corona Warn App is given. Next the key quality driver of the app will be described and evaluated based on the open source documentation provided. Concluding from those key quality driver, two quality scenarios are developed and described. Last, recommendations will be given, how to implement these scenarios by applying tactics from the book “Software architecture in Practice”.

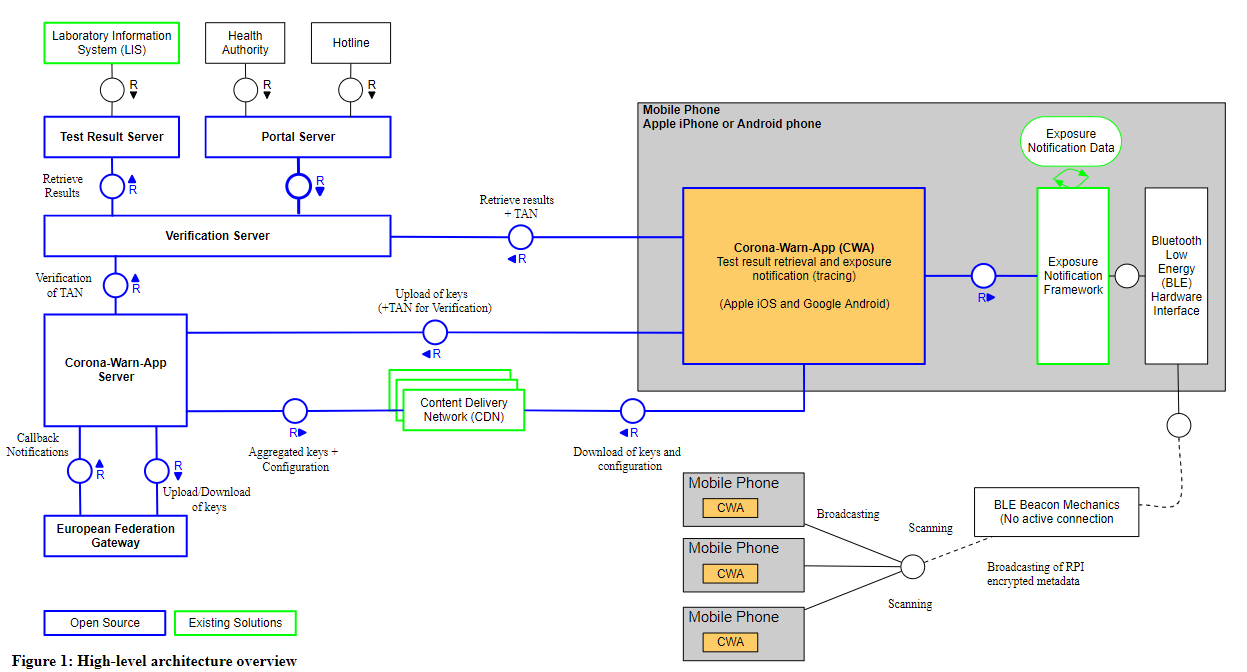
# Brief introduction to the Corona Warnapp

Figure 1 displays the high level architectural view of the corona warn app

https://www.bundesregierung.de/breg-de/themen/mythen-und-falschmeldungen/corona-app-falschmeldungen-1758136



Figure



# Relevant Quality Aspects of the German Corona Warnapp

In order to derive the key quality aspects associated with the German Corona Warnapp, the open source documentation is used, based on the version of the 20th June 2020. In the following two paragraphs the key quality aspects data privacy and accuracy are introduced.

## Data privacy

One of the main requirements dedicated to the CWA is data privacy (Criteria for the Evaluation of Contact Tracing Apps). The data privacy is implemented in accordance with the recommendation of the Chaos Computer Club, a German Club that gives Hacker a forum for collaboration, enabling transparency in the public IT sector (CCC). It provides six concepts relating to data privacy. In the following paragraphs each of those concepts is explained and its implementation in the CWA documented.

The first concept describes the **non-existence of a central entity to trust**. This means that no secret data is stored centrally on the server. All confidential information must be stored locally.. The CWA implements this concept by not sorting any confidential data on the CWA Server, but only locally on the devices of the user of the application. However, in order to trace back the potential exposures of the user, data of other users is needed. This is enabled by implementation of a rolling proximity identifiers (RPI) into a notification framework. These RPIs are also stored on the users device and can only be accessed with consent of the user.

The second concept targets **data economy**. This principle is not only recommended by CCC, but is also a regular requirement in accordance with the General Data Protection Regulation. It requires the application to limit its data requested to a minimum to function correctly. The CWA implements this by restricting the used data to the following.

\*\*\*Maybe include all data points if not 5 pages\*\*\*

The third concept entails **anonymity**. By not being identifiable, a user’s data privacy is further protected. This concept is implemented by the temporary exposure key (TEK) in the CWA by. Only with the TEK and the RPI, a user can be identified. These TEK stays solely on the device of the user and changes every day. The RPI has a changing interval of 10-20 minutes.

The fourth concepts describes **the non-creation of central movement or contact profiles**. The CWA follows this guideline by not providing location data or RPI to the server. Further no identification is required for the CWA.

**Unlinkability** is the fifth concept described. By not linking keys and user identities visible in the system. As described earlier, the TEKs and RPI’s are changed frequently and can only be used to identify identities conjointly. This implementation is adequately fulfilling the unlinkability requirement of the CCC.

Last, the **Unobservability of communication** concept is described. It targets communication security by not allowing malicious sources to observe the communication. This being achieved by the CWA by applying TLS encryption mechanisms.

## Accuracy

The second quality aspect which is subject to further analysis is the usability of the CWA. As described in the introduction, the CWA is a tool to indicate the potential threat of infection and is a voluntary service to the users to break the infection chain. In case of a shortcomings on the usability, various side effects could occur.

First, there will be a substantial misguiding on the users that are confronted with wrong warnings. Users receiving false positive warnings from the CWA are recommended to stay in voluntary quarantine without the empiric need for this. On the other hand false negatives are not being notified with a warning whilst having a high risk of infection. These users continue their social interaction with an increased risk of spread the SarsCov 19 virus. The anticipated outcome of the CWA is reversed for these users. Whilst CWA aims for a reduction of the SarsCov 19 spread, users with false negatives might have a higher amount of social interaction than people that have not downloaded the application. This is the case, when the user has a high degree of trust in the CWA and expects to not be infected unless the CWA notifies the user.

Secondly there is a moderate impact on the image of the application. The CWA only pursues its goal of diminishing the infection rate if it is downloaded by a significant amount of people (Corona-Warn-App: Downloads). This fact in combination with the voluntary download make it necessary to have satisfied users. If the CWA is not convenient for the users, they may not download it and therefore decrease the general use and efficiency of the CWA. If the warnings generated are false positives or false negatives, and the user is notified about the wrong warning, the trust and subsequently the user satisfaction is decreased. This might lead to a uninstall of the application, harming the general goal of the CWA.

# Quality Scenarios

In this chapter two quality scenarios are developed, targeting the data privacy and accuracy quality aspects described in the previous chapter.

1x Datenschutz/Sicherheit – DDOS – (p.15)

|  |  |
| --- | --- |
| **Portion of Scenario** |  |
| Source | An external person, group or organization, with the intend to exploit data with negative intend, tries to access the data provided from the CWA. |
| Stimulus | The attempt is being made in order to commercially or politically use the data that was being retrieved from the CWA. By hacking into the system, retrieving data and publishing those datapoints, a profound damage can be caused, leading to lower trust into both, the CWA and the political approach to stop the SarsCov19 virus. |
| Artifact | The System’s data, including all data points consumed or created. Special interest is existent with regards to the personal data (name, email address) and highly critical health data (Covid status). |
| Environment | A running and operational version of the CWA, with at least one user being registrated in the CWA. |
| Response | Token policy |
| Response  Measure | Token based measures  Measure of exposed data points to the central server |

1x Data Accuracy

|  |  |
| --- | --- |
| **Portion of Scenario** |  |
| Source | End User, who got diagnosed with an SarsCov19 infection by a medical institution or an authorized body for Coronatesting. |
| Stimulus | End user wants to register his infection in the CWA in order to inform other users, that have been in close proximity to him lately, that they have a high risk of being infected too. |
| Artifact | A running CWA which has been used the past days, to supply a benefit to other users that were in close proximity to the person infected. |
| Environment |  |
| Response |  |
| Response  Measure |  |

* Measure accuracy of technical implementation of CWA – not measuring quality of scoring scheme in application. (e.g. scoring scheme testing not relevant: <https://github.com/corona-warn-app/cwa-documentation/blob/master/2020_06_24_Corona_API_measurements.pdf> )

# Tactics to implement Quality Scenarios

Design patterns

# 

# References

**Websites:**

Chaos Computer Club

https://www.ccc.de/de/club

Corona Warnapp Documentation – backend-infrastructure-architecture

<https://github.com/corona-warn-app/cwa-documentation/blob/master/backend-infrastructure-architecture.pdf>

Corona Warnapp Documentation – Criteria for the Evaluation of Contact Tracing Apps

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

Google exposure notification API Testing

<https://github.com/corona-warn-app/cwa-documentation/blob/master/2020_06_24_Corona_API_measurements.pdf>

Corona-Warn-App: Downloads überschreiten 24-Millionen-Marke

https://www.connect.de/news/corona-warn-app-download-zahlen-3200860.html

# Appendices

**List of Appendices**

[**Appendix 1 Sprint Items** 18](#_Toc60402361)

[**Appendix 2 Databricks ETL** 18](#_Toc60402362)

[**Appendix 3 Exemplary Stored Procedure** 20](#_Toc60402363)

[**Appendix 4 ERM BA Wind Cockpit** 21](#_Toc60402364)

[**Appendix 5 Landing page BA Wind Cockpit** 21](#_Toc60402365)

[**Appendix 6 Authorization concept** 22](#_Toc60402366)

**Appendix 1 Sprint Items**

