

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 an analysis of the architecture of the Corona WarnApp (CWA), based on the key quality aspects.

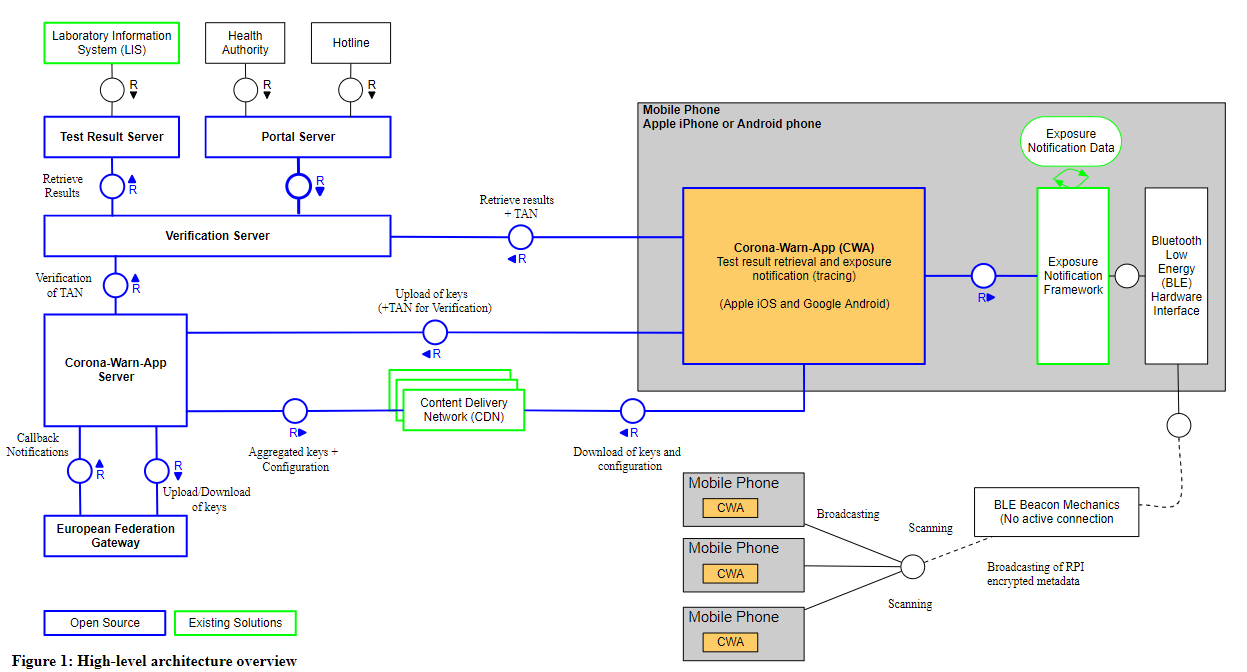
The report will proceed as follows. First, a brief introduction to the CWA is given. Next the key quality driver of the app will be described and evaluated based on the open source documentation provided. Concluding from those key quality driver, two quality scenarios are developed and described. Last, 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

The CWA is developed from SAP and Telekom in order to fight the spread of the Corona Virus. It is voluntarily and can be downloaded for free. Users of the application track their encounters with others and get notified if they have been in contact with a person who got infected with Corona. With this information, further spread of the potentially infected user of the CWA can be diminished.

Figure 1 displays the high level architectural view of the corona warn app. In general the application is divided into the CWA and various server components.

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.

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.

## Usability

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, 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 among all social classes and demographics. People that have very few experience with smartphone technologies (slate.com) need to be able to download and operate the CWA. If these users are overwhelmed by a complex setup and a low degree of usability, the application might not be kept on the phone. This point is gaining further importance when looking at the severity of Covid per age. It is stated that people over 65 have a 23 times greater risk of death compared to the under 65 years old people. Given this fact, old people have a higher need for protection from Covid and therefore need to be able to operate the CWA easily. Considering the example of an infection of a 70 year old person, a notification in the CWA might prevent other old people to get infected.

Due to these points, a low degree of usability would heavily harm the general goal of the CWA, to lower both, the infection rate and the ultimate deaths resulting from Covid.

# Quality Scenarios

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

Data Security – 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 | Defended attempt by blocking the intruder |
| Response  Measure | * Number of attempts that were not able to be blocked |

Usability quality scenario

|  |  |
| --- | --- |
| **Portion of Scenario** |  |
| Source | End User, with few experience with mobile applicaitons, 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 | The CWA Application that is running on the Smartphone of the enduser. |
| Environment | 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. Further it must be connected via internet to the server in order to supply the relevant information token to inform other users that have been in contact with the infected person. |
| Response | The application enables the user to update his infection status and notifies other users that have been in contact with this person. |
| Response  Measure | * % of users being able to update the infection status without help * Amount of time needed for this person to successfully update the infection status |

# Tactics to implement Quality Scenarios

After defining quality aspects in chapter two and deriving quality scenarios in chapter three, this chapter is about giving advices on how to enable these scenarios. Per quality scenario, two tactics are explained, that boost the quality aspect.

There is a wide range of tactics to implement data security. One of the tactics is part of the **tactics to resist** attacks. The tactic follows an approach to **detect the intruders**, in order to achieve both, resistance from the attack and learning from the attack to prevent further. It could be implemented in the CWA through extensive logging, which stores all requests made to central parts of the CWA. This would for instance include the Verification Server and CWA Server. In case an intruder is trying to access the server with malicious intent, the type of attack and the approach can be analyzed, and learnings can be generated from the persisted information about the attack .

The second example of a tactic to implement security is part of the attack reaction tactics. The **lock computer** tactic describes an tactic that automatically denies access to a certain resource if it has unsuccessfully tried to access the system various times. This mechanism assumes malicious and fraudulent access attempts behind multiple unsuccessful login attempts. By locking the resource, there is no opportunity to access the system for a defined timeslot. In case the unsuccessful attempts were made from a legimited person, further action for reactivation and new login attempts can be initiated. In the CWA this tactic could be implemented when registering as an infected status. The Code to register as corona infected could be tried to be hacked by iterating over possible combinations. By blocking the insertion after e.g. 3 wrong tries, the malicious attempt could be blocked.

Usability:

Next to the security tactics, there are also usability tactics, that enable achievement of the quality scenarios defined in chapter XY.

The first tactic to name is the **Cancel tactic** and is part of the tactics to **support user initiative**. This tactic stipulates the usability experience by giving continuous authority to the user. Processes that have been triggered by the user can be terminated at any time by the user. This allows a greater flexibility and a better perception of control, leading to a greater feeling of usability. Explicitly for the CWA, this means that for instance the lookup of the incidence figures can be terminated at any time for the user. This can be specifically convenient in case of poor connectivity, leading to long waiting times. Technically, this means that a listener element needs to be instantiating, allowing to terminate ongoing processes if needed.

The second tactic to name is the **Undo tactic** and is also part of the tactics to **support user initiative**. This tactic allows the user to undo the action that were triggered initially. This can be done by reverting the initial action. For the CWA this could be for example redoing the status entry.

# 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>

Why Older People Really Eschew Technology

<https://slate.com/technology/2020/07/seniors-technology-illiteracy-misconception-pandemic.html>

Journals:

Mueller, Amber L., Maeve S. McNamara, and David A. Sinclair. "Why does COVID-19 disproportionately affect older people?." *Aging (Albany NY)* 12.10 (2020): 9959.

# 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**

