Corona-Warn-App F.A.Q.

Version: 1 November 2021

Overview

The main points

The procedure

The technology

→ Bluetooth Low Energy is a very complex signal: how will measurements be made to ensure that only contacts within a certain distance are actually registered?
→ How well does the distance measurement work with Bluetooth and which tests have been carried out on this?
→ Is it really technically possible to identify chains of infection?
→ Why do we need a central server for a distributed solution? Isn't that a contradiction?
→ The Open Telekom Cloud (OTC) relies on technology from Huawei. Can you ensure that technologies from the Chinese manufacturer are not used in the central cloud system for the Corona-Warn-App?

The data

→ How are data security and data protection ensured for the Corona-Warn-App?
→ What personal data does the Corona-Warn-App store?
→ Why does the Corona-Warn-App use pseudonymisation and not anonymisation?
→ Can the Corona-Warn-App be used by authorities to monitor whether I am actually in quarantine?
→ Can children and adolescents use the Corona-Warn-App?
→ Doesn't the defined scope of services of the Corona-Warn-App also limit its effectiveness? Couldn't we achieve even greater effectiveness with more data?
→ Some virologists, if not many, would of course like to use the data collected by the Corona-Warn-App for their scientific research into the virus. This doesn't work to the desired extent with this distributed solution, or is there another approach possible?

Abroad

→ Can the Corona-Warn-App also be downloaded internationally and used on a cross-border basis? How do you ensure the interoperability of the Corona-Warn-App in Europe?

The parties involved

→ What contribution has the Robert Koch Institute made to the Corona-Warn-App?
→ What are the roles of SAP and Deutsche Telekom in this project?
→ What cooperation is there with Apple and Google?
→ Who runs the server to distribute the warnings / infection notifications?

→ Will the work carried out previously by the PEPP-PT organisation continue to be used in any form, or will everything be abandoned and started again from scratch?
→ Is the Fraunhofer Institute still involved?

The main points

Why do we need a Corona-Warn-App?

The app should help to curb the spread of COVID-19. It documents the digital encounter between two smartphones. This allows the app to quickly inform you if you had contact with a person diagnosed with COVID-19. The faster you receive this information, the lower the risk that many people will become infected. That is why the app is an effective means of curbing the corona virus, along with hygiene measures such as hand washing, social distancing and using everyday face masks. The Federal Government supports the app because it serves the protection and health of the community.

What does the Corona-Warn-App do?

The Corona-Warn-App informs you if you have been near a person for a longer period who is later diagnosed with the corona virus. This enables you to quickly react accordingly, and not run the risk of unknowingly continuing to spread the virus. The manual process of tracking infections will be greatly accelerated with this digital assistance. This is especially important when more people are meeting up, in order to curb the spread of the virus. The app runs on your smartphone while you go about your everyday activities. It recognises other smartphones nearby which also have the app enabled. The app then stores their random Bluetooth IDs (random IDs) for a limited period of time. These encrypted IDs (random IDs) do not allow connections to be made to you or your location. In addition, you can use the Corona-Warn-App to provide digital evidence of your vaccination status, save the result of a current rapid test and check in to an event with a QR code.

How does the Corona-Warn-App work?

The Corona-Warn-App uses Bluetooth technology to measure the distance and duration of the encounter between people who have installed the app. The smartphones "remember" encounters if the criteria determined by the RKI on distance and time are met. The devices then exchange random IDs. If people using the app test positive for the corona virus, they can inform other users on a voluntary basis. Then the random IDs of the person diagnosed with COVID-19 are made available to all people who are using the Corona-Warn-App. If you have installed the app, it will check whether you have had contact with the person diagnosed with COVID-19 for you. This check is only performed on your smartphone.

If it is positive, the app will display a warning. At no point in time does this procedure allow connections to be made to you or your location.

The app is currently available in the following six languages: German, English, Romanian, Bulgarian, Polish and Turkish. Am I obliged to use the Corona-Warn-App?

No. It is up to you to decide whether or not you want to use the app. Use of the Corona-Warn-App is voluntary, and is for your personal protection, as well as the protection of your fellow citizens. The aim of the Corona-Warn-App is to quickly identify and interrupt corona chains of infection. All users should be quickly and reliably informed about encounters with users of the app who have been diagnosed with COVID-19, and thus about a possible transmission of the virus. So they can quickly isolate themselves and get tested on a voluntary basis, and thereby help to curb the corona pandemic. You can disable the functions of the app at any time, or delete the app entirely. This will also delete all of the information stored by the app.

Since downloading and using the app is voluntary for citizens, there is no need for statutory regulation of the voluntary use of the app by the population. In the opinion of the Federal Government, compulsory use of the app by employers, shops or other persons would contradict the principles of the General Data Protection Regulation (GDPR). The app is neither intended nor suitable for the purpose of restricting access to facilities.

Why should I use the Corona-Warn-App?

If you use the app, you are making an active contribution to curbing the pandemic. The faster that people who have been diagnosed with COVID-19 and their contacts can be informed, the less the virus can spread. The app therefore helps you to protect yourself, your family, your friends and everyone around you. Without this technical assistance, staff at the health authorities would have to track each case personally.

This is very time consuming, and it is often not even possible to find every single person, because who remembers everyone they have had contact with? The Corona-Warn-App solves these problems.

Who is behind the Corona-Warn-App?

The Corona-Warn-App is a project commissioned by the Federal Government. The companies Deutsche Telekom and SAP have developed the application, based on a distributed software architecture. The Fraunhofer-Gesellschaft and the Helmholtz Center for Information Security (CISPA) provided advice and support. In order to meet the requirements for data protection and data security, the Federal Office for Information Security (BSI) and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) were also involved. The Robert Koch Institute plays a dual role in the Corona-Warn-App: it provides specialist expertise for the development of the app, and as publisher is also responsible for carefully checking the requirements for data protection and data security.

What are the minimum device requirements?

The Corona-Warn-App is designed to be completely accessible to all. As many citizens should be able to use the app as possible, in order to ensure maximum protection against a renewed rapid spread of the virus. Therefore, the app can be used on the vast majority of current devices and with the common operating systems. The required update to the relevant operating system (iOS, Android) is usually carried out automatically on your smartphone. The app runs on iOS smartphones from the iPhone 5s upwards using iOS 12.5, and on Android-based smartphones from Android 6 upwards.

More detailed information about the technical aspects can be found here:

https://www.coronawarn.app/de/faq/

What has improved with the updates?

As is the case with many other digital applications, the development of the Federal Government's Corona-Warn-App is not finished once it has been released, but it is a project which is constantly being worked on in order to correct any errors which occur and to make continual improvements.

The following page: https://www.coronawarn.app/de/ provides detailed information about all of the updates to the Corona-Warn-App.

The developers of the Federal Government's Corona-Warn-App will continue to incorporate suggestions which they receive via various channels into the app's updating process. You are welcome to read more about these developments or get involved:

https://github.com/corona-warn-app/ If you have any questions, please feel free to contact the technical hotline under 0800 7540001.

The procedure

When does the Corona-Warn-App actually warn users?

You will not receive a real-time warning if you come within two metres of a person diagnosed with COVID-19. The solution cannot enable a response in real time for data protection reasons. This would determine the identity of a person diagnosed with COVID-19 and violate corresponding protective rights. Your own smartphone has no information about who is infected. It only knows that it was near another smartphone on which a verified positive test result has been saved.

Each person alone decides if a positive test result is shared or not.

We are striving for an automated process where the result of "test positive" can be transferred to the smartphone as soon as it is reported and the person has actively authenticated themselves. However, every person who uses the app must always first manually change their status in the app to "positive" using a "sliding button". This kind of automated process is not yet possible today at all testing laboratories. In places where an automated process is still not possible, there is a manual process of calling an activation hotline to report positive tests, including verification of the test result.

Which criteria are used to assess potential exposures, and what are the different recommendations for action?

In order for an encounter to be rated as a potential exposure by the Corona-Warn-App, it must have been epidemiologically relevant. This means that there must have been a risk of infection. The Bluetooth technology used by the app allows it to work with two parameters: the duration of the encounter and the distance between the users. Both are calculated with the help of various measurements, and a threshold value is established.

When contact occurs, the relevant users exchange temporary random IDs. These random IDs are stored exclusively on the smartphones of the relevant users who encountered each other for 14 days, and are compared with so-called diagnosis keys of those who are diagnosed with COVID-19, directly on the person's smartphone.

Exposure is defined in the app as an encounter with a person diagnosed with COVID-19, who exceeds a threshold value of various measurements. The people using the app are shown their risk status depending on these measurements.

There are three types of status information:

low risk:

- The person is informed that the exposure check of their exposure logging has shown no encounter with anyone who is known to have been diagnosed with COVID-19, or that any such encounters did not exceed the defined threshold value.
- The person is informed about generally applicable social distancing regulations and hygiene recommendations.

increased risk:

- The person is informed that the exposure check of their exposure logging has shown an increased risk of infection, as they have encountered at least one person in the last 14 days who has been diagnosed with COVID-19.
- The person receives the recommended action to, if possible, go straight home or stay at home, as well as to contact either their general practitioner, the medical assistance hotline at 116 117 or the local health authorities and discuss the further course of action.

unknown risk:

- If the risk identification has not been activated for long enough by the person, then no risk of infection can be calculated at this time. The person receives the status information "unknown risk".
- Risk identification is possible within 24 hours of installation, at which point the status information displayed changes from "unknown risk" to "low risk" or "increased risk".

More detailed information about COVID-19 can be found here:
https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/nCoV.html

Is the "increased risk" warning by the Corona-Warn-App enough for sick leave or ordering quarantine?

The "increased risk" warning by the Corona-Warn-App only informs the user that the close proximity and duration of an encounter with a person who has reported a positive test result via the app means that there is an increased risk of infection, and recommends that the user contact either their general practitioner, the medical assistance hotline at 116 117 or the local health authorities by telephone.
The decisions on a medical certificate for sick leave and on ordering isolation at home (quarantine) are made by the consulting doctor and the relevant health authorities after an appropriate assessment.

Contact tracing in the event of an infection is the task of the health authorities. How do "traditional" contact tracing and the Corona-Warn-App work together?

The health authorities use information provided by the person diagnosed with COVID-19 to identify the people who have been in contact with that person, in order to curb the spread of the virus. The Corona-Warn-App is an important supplement to these efforts, because it helps to identify exposures in addition to the health authorities:

– encounters with unknown people in public will also be recorded and
– identified faster, because this is done automatically in the Corona-Warn-App.

If a user of the app receives a warning that they have had a relevant encounter with a person diagnosed with COVID-19, recommendations on what to do will be given to them, such as contacting either their general practitioner or the health authorities, and/or voluntary isolation at home.

Contact tracing by the health authorities remains necessary, e.g. to identify or inform people who are not using the app or don’t have a smartphone. Of course, contact tracing and notification via the app also does not replace the notification channels prescribed in the Infection Protection Act (IfSG).

Can the Corona-Warn-App protect me from contact with people who have been diagnosed with COVID-19?

No, the app cannot predict such contacts, and for data protection reasons also doesn’t report in real time, whether for example there is an infected person in a

supermarket. This is why wearing a face mask covering the mouth and nose also remains important. The Corona-Warn-App estimates a delay of approximately half a day up to a full day before positive test results are displayed via the app. Thus, real-time protection cannot be ensured.

What happens if I have two smartphones? Do I have to download the Corona-Warn-App on both?

For the technology to be effective, it is crucial that you have a smartphone with the app on it when you are out in public.

The use of a second device does not alter this effectiveness. But as a matter of principle, no information can be exchanged or synchronised between the devices - each additional smartphone is technically treated like that of a stranger.

The technology

What are the prerequisites for the Corona-Warn-App to work correctly?

You will be informed by the app if a prerequisite is not currently being met. The Bluetooth function must be activated continuously in order to enable the exchange of pseudonymised contacts to other app users. The camera on the phone must be functional in order to scan the QR code for verification of the test results of your COVID-19 test. There must be an active Internet connection at regular intervals (ideally as often as possible), to obtain up-to-date information about personal risk from contacts, and to make the risks posed by your own COVID-19 infection visible to other app users. The data protection policy must be agreed to.

How will the Corona-Warn-App work in future with smartphones from Huawei or others which do not run on the iOS or Android operating systems?

In principle, we are developing the solution for iOS and Android operating systems. The most common phone types are certainly taken into account while developing the solution.

How does using the Corona-Warn-App affect the battery life and storage space of smartphones?

The application runs in battery-saving background mode. When developing the solutions, we of course pay special attention to minimising the storage space required for the app itself and the contact with other smartphones stored.

Are there storage requirements for the smartphone?

The Corona-Warn-App will require less than 20 MB of storage space on the phone. The exact size can be determined after the launch date, and may also change due to possible updates (although this change in size should be minimal). In addition, extra storage capacity is required for the data recorded temporarily by the app.

Bluetooth Low Energy is a very complex signal: how will measurements be made to ensure that only contacts within a certain distance are actually registered?

The Fraunhofer-Gesellschaft is assisting the project consortium led by SAP and Deutsche Telekom with the development of the app. In particular, the Fraunhofer Institute for Integrated Circuits IIS is closely involved in specific technological challenges, for example the optimisation and efficient use of the underlying Bluetooth technology for distance measurement. The researchers at the Fraunhofer IIS are contributing their long-standing know-how in distance estimation with moving devices/people via signal exchange between devices using the Bluetooth Low Energy (BLE) standard. Field trials are currently underway in simulated everyday situations.

How well does the distance measurement work with Bluetooth and which tests have been carried out on this?

As part of tests of the interface to Google/Apple (so-called exposure notification interface) for the Corona-Warn-App, numerous tests were carried out over the past few days at the Fraunhofer IIS and discussions were held with SAP, Telekom and the RKI, plus the configuration of the CWA was jointly adapted with the RKI. The aim of the test was to check how accurately the Google/Apple interface can estimate the duration of an encounter and the distance between smartphones in various scenarios (on the train, queues at the supermarket, restaurants, parties) according to the RKI's specifications. The basis of these specifications is an

epidemiological model by the RKI which determines as from which duration and which proximity an encounter can be classed as epidemiologically critical.

From the results of the tests, we can say that around 80 percent of the encounters were correctly recorded in the last test series, using various mobile phones in the investigated scenarios. Over the next few weeks, we will perform more tests to constantly improve the accuracy of the CWA. To do so, SAP, Telekom, Fraunhofer and the RKI are working closely together, and are also collaborating with Google and Apple to adapt the interface.

Is it really technically possible to identify chains of infection?

For this purpose, the Corona-Warn-App uses Bluetooth Low Energy technology to measure the distance between people, and enable the smartphones to record the contacts which meet the criteria (distance and time) determined by the RKI. When doing so, the phones exchange temporary encrypted random IDs. If users of the Corona-Warn-App are diagnosed with COVID-19, they can voluntarily let the app inform people they have had contact with. In the event of an infection, the encrypted random IDs of the infected person are made available to all the mobile phones of the active app users. These phones can then check to see if they had contact with the IDs provided. If a match is found, the user is warned about the exposure.

Why do we need a central server for a distributed solution? Isn’t that a contradiction?

No, it isn't. The server only has the task of safely and efficiently sending the pseudonymised and authorised positive reports to all participants, so that an exposure check can take place on the users’ end devices, so locally. Of course no data is stored centrally above and beyond this.

The Open Telekom Cloud (OTC) relies on technology from Huawei. Can you ensure that technologies from the Chinese manufacturer are not used in the central cloud system for the Corona-Warn-App?

The OTC uses Openstack in the central core. Openstack is an open source technology that is developed by a global community with full transparency, and is written in Python. Python is a scripting language, and the software is thus used in all critical parts of the source code. We therefore have transparency about what

happens and what is executed in the core of our cloud. Huawei is the supplier of the technical platform, but has no administrative access to the OTC.

All administrative tasks are carried out entirely by T-Systems staff.

The data

How are data security and data protection ensured for the Corona-Warn-App?

The protection of your privacy is a top priority for the Federal Government. Therefore, when the Corona-Warn-App was being developed, it was ensured that the app meets the stringent German data protection requirements. In order to ensure that these requirements are met, both the Federal Commissioner for Data Protection and Freedom of Information (BfDI) and the Federal Office for Information Security (BSI) were involved in the development of the Corona-Warn-App right from the beginning. The BSI supports the development of the app on matters related to IT security. The BSI was therefore constantly examining the versions of the app provided by the developer teams during the development process, as well as the associated infrastructure, and providing advice on the security concept to be created. In addition, the complete source code on which the app is based has been made available to the public. This allows independent specialists from civil society to participate in the development and improvement of the app at any time, and to check it for weaknesses.

More detailed information about data protection and IT security can be found here: https://www.coronawarn.app/de/faq/

What personal data does the Corona-Warn-App store?

Your data is safe at all times. When you use the app, you will remain anonymous at all times. When you register to use the app, you do not have to provide any personal data (such as your name or e-mail address). The distributed data storage on the user devices themselves, as well as full pseudonymisation, guarantee a high level of data protection. All data – for example on encounters with other people using the app – is encrypted and stored exclusively on your own smartphone.

Temporary random IDs are saved of other smartphones which have the app installed on them, if the RKI's epidemiological criteria for the proximity and

duration of an encounter are met. In the event of an infection, your own random IDs can be voluntarily shared, which enables other app users to have their risk calculated on their smartphones. With this data and the locally-stored data, it is possible for the app/smartphone (but not the server) to identify contact with a person diagnosed with COVID-19, and to warn the person accordingly. Data which can make a person identifiable, in particular location data, is not selected, used or stored. It is ensured that a person diagnosed with COVID-19 does not know which people are informed about an encounter. Contact people do not receive any information about the person diagnosed with COVID-19. Falsely reporting the infection status is prevented by technical and organisational measures. Neither the Federal Government, the Robert Koch Institute, nor other people using the app or the operators of the app stores can detect whether you report an infection with corona yourself, or whether you have had contact with a person diagnosed with COVID-19.

Why does the Corona-Warn-App use pseudonymisation and not anonymisation?

The tracing in the app can logically only take place by pseudonymisation, otherwise no warning to other users would be possible. This also ensures protection against misuse of the app: to verify an infection, test results and specific smartphones – but not specific people – must be able to be safely matched with each other. While tracing, Bluetooth keys are used which change every 10 minutes. Bluetooth keys are pseudonyms which are changed at short intervals, to make identification of individual pseudonyms even more difficult. The user does not have to enter any personal data in the app. It is only possible for the users themselves to identify the personal reference.

Can the Corona-Warn-App be used by authorities to monitor whether I am actually in quarantine?

No, this is not technically possible. It is also not envisaged in this app in future.

Can children and adolescents use the Corona-Warn-App?

In principle, the Corona-Warn-App can be obtained via the relevant app stores by anyone aged 16 and older. Children and young people under the age of 16 can use the app if they have discussed this with their parent/guardian and obtained

consent. We recommend that you use appropriate child protection mechanisms when downloading apps (e.g. those of the platform provider or a secure third party). As a parent/guardian you can configure child protection mechanisms so that children and young people can only download programmes which are suitable for them.

When installing the Corona-Warn-App, as well as before you upload a positive test result in the app, you will be notified that use of the app by children and young people under the age of 16 is only permitted with the prior consent of their parent/guardian.

Doesn't the defined scope of services of the Corona-Warn-App also limit its effectiveness? Couldn't we achieve even greater effectiveness with more data?

We are developing an app that is limited in its scope of services to the important task of informing citizens about possible risks of infection. We are convinced that this is a prerequisite for maximum acceptance and participation.

Some virologists, if not many, would of course like to use the data collected by the Corona-Warn-App for their scientific research into the virus. This doesn't work to the desired extent with this distributed solution, or is there another approach possible?

Value-added services and data collection beyond the agreed purpose of the app are excluded. For us, the most important challenge is to improve and accelerate tracing of contact chains using digital means. Our application focusses on this objective.

Abroad

Can the Corona-Warn-App also be downloaded internationally and used on a cross-border basis? How do you ensure the interoperability of the Corona-Warn-App in Europe?

Currently, most corona warning apps are only available in the respective app stores of each country. This is due to the fact that the app users mostly live in the respective country. Also, the processes behind the app, including those related to testing, are based on the respective national health structures.

The Federal Government's Corona-Warn-App is now available to download in all national app stores in the European Union, as well as those in Switzerland, Norway, Great Britain and Turkey.

In October 2020, upon suggestion by the EU member states, the European Commission set up an EU-wide system for the interoperability of various corona warning apps in Europe. With this system, some European corona warning apps are able to communicate with each other across country borders and exchange warnings. The European gateway server required to use the Corona-Warn-App across borders has been installed by T-Systems and SAP on behalf of the European Commission.

The countries which are already connected to the European gateway server can be found here:

Open source project for the Corona-Warn-App – FAQ

The following also applies for this European system: no additional information will be processed other than the random IDs generated by the apps. The information will be exchanged by pseudonymisation and encrypted, and remains restricted to the minimum amount necessary. All data will only be stored for as long as is necessary to trace infections. The identification of individual people is just as impossible to do as locating or tracking the movements of devices.

The parties involved

What contribution has the Robert Koch Institute made to the Corona-Warn-App?

The Robert Koch Institute plays a dual role in the Corona-Warn-App: it provides specialist expertise for the development of the app, and as publisher is also responsible for carefully checking the requirements for data protection and data security.

During the development of the app, the Robert Koch Institute contributed its scientific expertise on how encounters during which there was a risk of infection ("epidemiologically relevant contact") are categorised by the app, and on which measures are advised for users of the app in the event of an encounter with a person who tested positive for SARS-CoV-2.

What are the roles of SAP and Deutsche Telekom in this project?

Since the end of April, a joint team from Deutsche Telekom and SAP has been working on the Corona-Warn-App, which is designed as an open-source solution. SAP provides the required software technology via a technical platform, and promotes the development of the solution. Deutsche Telekom provides its expertise in processes related to network and mobile phone technology, systems integration and data security, and ensures safe and efficient operation.

What cooperation is there with Apple and Google?

Apple and Google provide a uniform standard for the Bluetooth distance measurement used. For example, previous tracing apps were limited because Apple simply prohibited the tracing in passive mode in its operating system. In addition, the cooperation ensures that smartphones using both operating systems – i.e. iOS for Apple and Android for Google – can communicate seamlessly with each other, and that the application can run in the background in battery-saving mode. Due to their market share of 99%, a standardised protocol is essential, especially for compatible use in Europe as well. The national apps rely on this basic functionality.

Who runs the server to distribute the warnings / infection notifications?

The “server” is made available and run by T-Systems. We provide this service from a data centre in Germany.

Will the work carried out previously by the PEPP-PT organisation continue to be used in any form, or will everything be abandoned and started again from scratch?

The underlying distributed approach now adopted was also always considered by PEPP-PT as a potential option. Important preparations have also been carried out and findings have been made, especially with regard to the distance measurements when using the Bluetooth Low Energy function.

Is the Fraunhofer Institute still involved?

The Fraunhofer-Gesellschaft and the Helmholtz Center for Information Security (CISPA) are providing advice and support with the app’s development. We are especially reliant on close cooperation with leading research institutions for challenges which require intensive scientific involvement, such as the interplay of technology and epidemiology. Fraunhofer is an important partner for us,

particularly for optimisation of the underlying Bluetooth technology. In precisely this area, Germany has helped tackle the global challenge through valuable research this year.