QRONITON

Secure contact tracing with QR codes

QRONITON is a contact tracing service with which institutions can fulfill their documentation obligation in the fight against pandemics and health authorities can quickly locate persons at risk. The browser-based web solution works with QR codes, simplifies contact tracing and consistently protects users' personal data against misuse.

The IT service was developed in cooperation with health authorities and the Robert Koch Institute and satisfies the most stringent data protection requirements. The users' contact data and the contact chains collected using scans are multiple-encrypted and remain inaccessible until concrete cases of infection occur. A time- and location-dependent encryption system ensures that only the contact data for directly affected users at serious risk of infection can be viewed and forwarded to the health authorities.

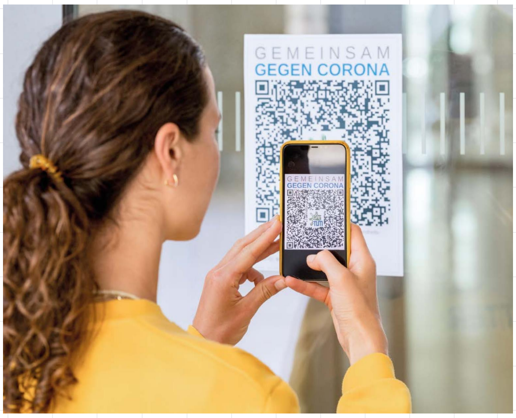


Photo: Astrid Eckert / TUM

While using the IT service, in general only as little personal data is collected as is absolutely necessary to deal with the Corona crisis. Personal data is processed and passed on exclusively as part of this explicitly social purpose and in compliance with all applicable legal provisions. Under no circumstances will personal data be passed on to unauthorized third parties, i.e. to third parties outside the responsibility of the operator or the healthcare system. In the course of an external audit of the solution, order data processing with QRONITON was classified as harmless.

The encryption technology used is based on the latest state of the art technology and precludes data misuse and manipulation. The concept is extremely robust against illegitimate access attempts – in particular by the parties involved themselves. Access to unencrypted data by the IT service operator remains barred at all times. Numerous security mechanisms prevent errors in use and targeted attacks by outsiders. The encryption concept has been verified by independent cryptologists and further audits are possible at any time by disclosing the source code.

Contents

This document describes in a comprehensible manner for any interested party the data protection-related processes in QRONITON when collecting and tracing contact chains.

Data collection

Personal data

In the course of initial use, the user's telephone number and name are queried or – if the university so wishes – linked to the user's user ID via an external campus login. From the data provided, a user key for the encryption of contact scans is derived, which can be reconstructed by the university in case of infection and used as an entry point for contact tracing. For the purposes of a risk assessment by the responsible health authorities, the user is also asked for a postcode or year of birth – invariably on a voluntary basis. All personal data is encrypted directly on the user's device or browser and then transmitted to the operator's infrastructure. On request from the user, registration data can also be secured against misuse with a PIN code. For statistical-epidemiological purposes and to improve the service, postal code and/or year of birth (if given) are transmitted in a form accessible to the operator. All other data points collected can only be decrypted by the key of the university and remain permanently inaccessible to the operator. The option for offline participation by generating an explicit personalized QR code is also available to every user. Digital QR codes for spontaneous meetings, valid for 24 hours, can also be generated via the web application. In both variants, the encoded transmitted registration data of the user is linked with the data of the respective QR code without any possibility for the operator to refer back to it, i.e. also encoded.

Location-related data

A user group authorized by the university also has the option to generate location-related QR codes. During this process, location-typical data, such as postal code, building and description are queried. Location-related QR codes include the specified location data in their embedded web URL for display during scanning. When generating the QR codes, the corresponding data is encrypted on the user's device in a similar way to personal data and transmitted to the operator's infrastructure without being personalized. For statistical-epidemiological purposes and to improve the service, the postal code of the location is made accessible to the operator. Conclusions concerning individuals or concrete buildings remain barred for the operator.

Contact recording by means of scans

By scanning a QR code, the relevant user's personal data is linked with the personal or location-related data for the scanned QR code. During this, a time stamp accurate to the nearest second is generated and the expected duration and intensity of the contact is queried via a selection list. In the resulting data record, references, inaccessible for the operator, to the encrypted data of the scanning user and the encrypted location data in the QR code are transmitted. These references are secured with the university key, as well as with a time/location-dependent code valid for 30 minutes, which itself is encrypted with the user key and also transmitted. For statistical-epidemiological purposes, anonymous scan information, i.e. contact duration and contact intensity, as well as the location postal code, are also transmitted in a manner accessible for the operator.

Linking contact scans

Several users at the same time and in the same location use the same time/location-dependent key for encryption of scan data and store this securely with their user key in the resulting data records. After reconstruction of a user key by the university in case of infection, all time/location-dependent keys used by the affected user make the scan data of direct contacts with shared stays become accessible. The references contained therein to encrypted user and location data can be reconstructed in a further step using the university key. Further stays of affected users that are not connected with the infection event, however, remain inaccessible, as these were collected with another, unknown time/location-dependent key.

Data storage

Provision on user devices

The key and control data required by the web application, without a personal reference, are stored on the user's end device, i.e. in the user's persistent browser memory. If specified, the user's postal code is also stored, in order to be able to encrypt the data records collected not only with the university key but also with the key of the health authority responsible for the user's place of residence. In addition, information on the last scanned QR code is stored as evidence of the scan. For information purposes, the total number of all scanned QR codes, as well as average values over 14 days for the number of contacts and contact hours are also stored and continuously updated on the user's device. None of this information is transmitted to the operator, nor is it possible to draw conclusions about previously visited locations. Upon the user's request, the stored statistical data can be reset or completely deactivated at any time.

Transfer to the operator's infrastructure

Each data record transmitted to the operator's infrastructure is encrypted not only with the university key and any other time/location-dependent keys, but also with an additional key from the operator, so that only indistinguishable data records are transmitted and the use of a cloud provider to accept the data is possible without risk. The partial decryption of the data records by the operator takes place in their own infrastructure on specially secured systems. Moreover, every form of data transmission is also secured with an additional transport encryption. Basically, provision of personal scan data in the operator's IT infrastructure is limited to 28 days; older contact scans are deleted continuously.

Data provision without unique identifiers

In the transmitted data records, there are no identifiers or consistent characteristics accessible for the operator, from which a movement profile – even in pseudonymous form – could be derived. This is guaranteed by a consistent decoupling of registered user and location data from continuously collected scan data via encrypted references, as well as by an ongoing time/location-dependent re-encryption of the corresponding scan data before every transmission. Due to a random component embedded in the encryption technology, successive scans of individual users cannot be assigned to them.

Consent to the collection of data

On calling up the web application, no personal data is generated or collected without the user's consent. In particular, no server logs are kept or IP addresses of the caller are logged. The use of web analysis services of third parties, advertising material or other forms of visitor-based monetization as well as the integration of external source material is completely avoided. Personal data will only be collected with the express consent of the user during registration. With each scan process carried out by the user, a time/location-limited consent to the use of personal data in case of infection is given, which can be revoked in accordance with the German Law on the Prevention and Control of Infectious Diseases with a period of notice of four weeks by calling up a corresponding function in the web application. The operator also undertakes to continuously delete all scan data collected after 4 weeks. At the user's discretion, data stored locally in the browser memory can be deleted at any time using the corresponding function in the web application or by clearing the browser storage.

Data processing

Operator

The generation of anonymous QR Code URLs and time-dependent key components is centralized on dedicated server systems, while location-dependent key components for storage in the QR Code URLs are generated locally on the devices of the respective users. No information is stored or logged on these key servers, in particular identifiers, key components, IP addresses or even concrete times of key generation. All data processed is stored exclusively as volatile in the main memory of the server systems and is not correlated with the encrypted user or location data collected. The operator undertakes to implement these measures permanently. Irrespective of this, an unauthorized collection of corresponding server protocols would not lead to a weakening of the data protection concept due to the consistent use of additional key components that are always inaccessible to the operator. Trust in the integrity of the operator infrastructure is therefore generally not necessary. The receipt of encrypted personal and location-related data as well as scan-based contact references is realized via independent server systems of the operator, which do not have any communication channels to the key servers. Since the present data protection concept only provides for the transmission of multiple encrypted data records, which can only be decrypted selectively in case of infection and in cooperation between the university and the operator, there are no security-relevant concerns for the server infrastructure of the operator. The use of a cloud provider based in Germany is therefore not critical for these purposes. The initial decryption of the received data records by the operator, i.e. the generation and processing of statistical information, takes place exclusively on the operator's own systems in its own infrastructure, which is located in a secured data center in Frankfurt. The same applies to the delivery of the data records (still encrypted with the university key) to the person in charge of the university in the context of contact tracing in case of infection.

University

Those responsible at the university can use the telephone number or campus ID of an infected person to reconstruct their user key and use it to trigger infection tracing. Subsequently, the operator returns the registration data encrypted with the university key to the browser of the responsible person and decrypts it there. The correctness of the contact data stored for the user key must be verified and confirmed by the responsible person. Using the scan keys of the affected user identified, all contact scans of persons at the same time and at the same place are then found, returned and also decrypted in the browser of the person responsible. The final step is the delivery and decryption of the registration data of all identified contact persons. In order to prevent misuse, a unique authorization code can be derived from this data, which is individual for each user and is also available to the users concerned in the web application. By comparing the authorization code, the affected user can legitimize the contact of the responsible person. In addition, the responsible person himself or herself has access to checksums of the registered user and location data as well as the PIN codes (if assigned) entered by the users during registration and scanning processes, which can be used to reliably detect misuse of contact recording by third parties. At no time does the operator gain access to decrypted data records of any kind, but logs the time of each tracking request to prevent misuse by the university.

Health authorities

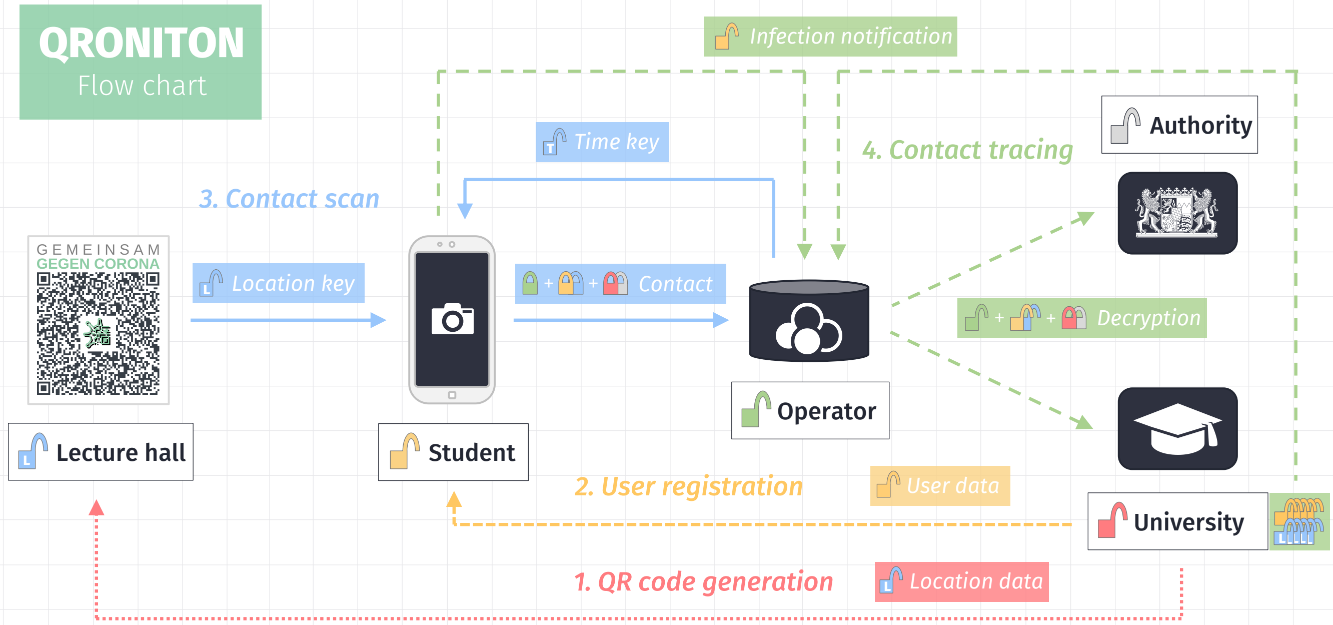
The contact details of users directly affected by the tracking are, by their very nature, intended for disclosure to the relevant health authorities. Based on the postal code of the respective users (if specified), the contact data can be distributed in a targeted manner. Otherwise it will be forwarded to the competent authority at the university location. If the university wishes, direct access for health authorities can also be set up. In this case, all collected data, i.e. registration information for users and locations as well as contact scans, are secured with the key of the university as well as the key of the competent authority. This key is determined on the basis of the postal code, so that affiliated authorities can only decrypt data records in their area of responsibility. All security guarantees, especially with regard to purely case-related data access for the protection of uninvolved users and user stays, remain valid.

Epidemiologists

For statistical purposes, in particular to monitor the effectiveness of containment measures, as well as for the purpose of further research on the spread of the corona virus, completely anonymized, i.e. location-related aggregated data records without any personal reference are generated. These data records are used by the operator to improve the service and are passed on to authorized bodies, e.g. epidemiologists or research institutes designated by the Robert Koch Institute. Correspondingly passed on data contains only aggregated information by postal code. With the help of this research data, an anonymous evaluation of contact clusters, regional accumulations, spread patterns, etc. is possible without drawing conclusions about individual users and thus improving pandemic control.

Encryption concept

In the course of the initial setup, a university certificate [🔒] is generated for the encryption of user data in QRONITON, optionally supplemented by a further system access for the local health authority [🔒]. Any transmission of data to the QRONITON infrastructure is always secured against data theft and manipulation with a certificate of the operator [🔒]. All certificates are delivered to the respective actors when the web application is called up. The following diagram shows the corresponding processes of the QRONITON service in the university environment.



Step 1: QR code generation

A unique web URL is retrieved from the operator for embedding in the QR Code. In the browser, the responsible person enters location data to describe the event or room, generates a random location key [🔒] and attaches it as a URL fragment (#). The location data is encrypted asymmetrically with the certificates [🔒] and transmitted to the operator.

Step 2: User registration

A user key [🔒] is generated in the user's browser from user data retrieved from the university (or manually entered) and stored locally in the user's browser storage. The user data is encrypted asymmetrically with the certificates [🔒] and transmitted to the operator.

Step 3: Contact scan

By scanning a QR code the web application is called up. From the URL fragment the location key [🔒] is extracted on the device but not transferred to the web application. In addition, time keys [🔒] for the QR code are retrieved from the operator for each 30-minute interval of the selected length of stay. The combination of both keys results in time/location-dependent composite keys [🔒], which are identical for all simultaneous contact scans of a specific QR code. These composite keys are used to symmetrically encrypt references to the registered user and location data. The composite keys themselves are also symmetrically encrypted with the user key [🔒]. All encrypted data points are transmitted to the operator together with the user data for the scan (time, duration, intensity).

Step 4: Tracing

To trigger the contact tracing, a concrete user key [🔓] is transmitted by the user or the university. This enables the identification and decryption of all time/location-dependent composite keys [🔓] that have been used with the user's contact scans. This in turn can also be used to decrypt all other contact data records of other users protected with these keys. The resulting accessible user and location data of all contact persons are transmitted (still asymmetrically encrypted) to the university or authority, which decrypts them with the private key of their certificate [🔓|🔓] in the browser.

Encryption technology (appendix)

The crypto-primitives and encryption technology described below are used as part of every data collection and data processing in the QRONITON service.

Symmetric encryption

A randomly generated key of length 128 bits and AES-GCM, i.e. Authenticated Encryption with Associated Data (AEAD), with a nonce of length 96 bits and a Message Authentication Code (tag) of length 128 bits is used. The parameters of the encryption as well as its results are transmitted to the operator's infrastructure in byte-coded form given as nonce|ciphertext|tag.

Asymmetric encryption

Public keys are available as X.509 certificates with 2048 bits key length. All data to be encrypted with these certificates is first symmetrically encrypted with a pseudo-randomly generated key using AES-GCM, i.e. Authenticated Encryption with Associated Data (AEAD). The key length is 128 bits. In addition, a nonce of length 96 bits and a Message Authentication Code (tag) of length 128 bits is used. The asymmetric RSA encryption of the symmetric key is done using RSAES-OAEP, i.e. using the Optimal Asymmetric Encryption Scheme according to RFC8017. SHA-256 (SHA-2) is used as the hash algorithm. MGF1 is used with SHA-256 (SHA-2) as well for mask generation. Correspondingly encrypted data is generated according to CMS/PKCS#7, i.e. conforming to the Cryptographic Message Syntax according to RFC5083 and RFC5084 and finally DER-coded in ASN.1 format and transmitted to the infrastructure of the operator. Within the scope of encryption, all recommendations of the current state of the art according to RFC6160 are implemented.

Key generation

The Key Derivation Function PBKDF2 with 100,000 iterations is used to generate symmetric keys of length 128 bits from user data (entered or retrieved via an Identity Management System). A salt is not used due to the lack of a source.

Transport encryption

Every form of data transmission is generally secured by TLS transport encryption. Older SSL versions are not permitted in communication. The X.509 certificate used is regenerated at short intervals. Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) with the curves X25519, P-256, P-384 and P-521 is the preferred choice for key exchange during connection setup. HTTP Strict Transport Security (HSTS) with a minimum duration of two years is used for all users of the web application.

Contact

If you have any questions, suggestions or problems, please do not hesitate to contact us. We will be happy to take care of your request and will be at your disposal with words and deeds.

Dr. Johann **SCHLAMP**	
schlamp@leitwert.net	email
F958 5A39 FCDC 383E E007 A911 E6CC 7F59 8B24 15A9	pgp
+49 841 93768493	phone
+49 174 4944947	mobile
Leitwert GmbH Donaustrasse 17 85049 Ingolstadt	address
GERMANY	

GEMEINSAM
GEGEN CORONA

https://qroniton.eu