QRONITON

Secure Contact Tracing with QR Codes

QRONITON is a contact tracing service to help institutions fulfill their obligatory documentation requirement in the fight against the pandemic and quickly locate persons at risk. The web-based 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. It meets the highest data protection standards. User contact data and the chains of transmission recorded via scans are encrypted multiple times and remain inaccessible until an actual case of infection occurs. Time/location-dependent encryption ensures that only the contact data of directly affected users with an acute risk of infection is accessible and can be forwarded to health authorities.

When using this IT service, as little personal data as absolutely necessary is collected in order to deal with the corona crisis. Personal data is processed and passed on exclusively within the scope of this explicit societal purpose and in compliance with all applicable legal provisions. Under no circumstances will personal data be disclosed to unauthorized third parties, i.e. to third parties outside the responsibility of the operator or the health care system. An external examination of the IT Service classified the order data processing with QRONITON as safe.

The encryption techniques are based on the latest technology and preclude misuse and manipulation of data. The concept is extremely robust against illegitimate access attempts—especially by the parties involved themselves. Access to unencrypted data by the operator of the IT service is not possible at any time. Application errors and targeted attacks by outsiders are prevented by numerous security mechanisms. The encryption concept has been verified by independent cryptologists; by disclosing the source code, further audits are possible at any time.

This document describes the data protection relevant processes in QRONITON for the collection and tracing of contact chains in a way that is comprehensible for everyone interested.

Collection of Data

Personal Data

When first using the service, the user's telephone number and user ID are connected 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 a starting point for contact tracing. For the purpose of a risk assessment by the responsible health authorities, the user is also asked to provide a postal code on a voluntary basis. All personal data is encrypted directly on the user's device or browser and then transmitted to the provider’s infrastructure. At the user's request, registration data can also be protected against misuse with a PIN code.

For statistical-epidemiological purposes and to improve the service, the postal code (if specified) is transmitted with the data, accessible to the provider. All other collected data points can only be decrypted by the university key and remain permanently inaccessible to the provider. Each user is also free to participate offline by generating a printable personalized QR code. The web application can also be used to generate digital QR codes for spontaneous meetings with a validity of 24 hours. In both variants, the user's registration data, which is transmitted in encrypted form, is linked with the data of the respective QR code without any possibility for the provider to refer back to it, i.e. it is also encrypted.

Location Data

For a user group authorized by the university, the generation of location-specific QR codes is also available. Here, location-typical data, such as postal code, building and description, are retrieved. Location-specific QR codes contain the location data in the embedded web URL for display during scanning processes. When generating QR codes, corresponding data is encrypted directly on the user's device in the same way as personal data and is transmitted to the provider’s infrastructure without any personal reference. For statistical-epidemiological purposes and to improve the service, the postal code of the location is made available to the provider. Conclusions about persons or specific buildings are not possible for the operator.

Contact Tracing by Scans

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

Connecting Contact Scans

Multiple users at the same time and place use the same time/place-dependent key to encrypt scan data and store it securely in the resulting data records with their user key. After reconstruction of a user key by the university in case of infection, all time/location dependent keys used by the affected user and the scan data of direct contact persons with shared stays become accessible. The references to encrypted user and location data contained therein can be reconstructed in a further step using the university key. Further stays of affected users who are not connected to the case of infection, however, remain inaccessible because they were collected with other, unknown time/location-dependent keys.

Data Storage

Storage on User Devices

The key and control data required by the web application are stored on the user's device, i.e. in the user's persistent browser memory, without personal reference. If specified, the postal code of the user is also stored, in order to be able to encrypt the data records 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 QR code scanned is stored as proof of scanning. For information purposes, the total number of all scanned QR Codes as well as average values over 14 days for the number of contact persons and contact hours are also stored and continuously updated on the user's device. This information is not transferred to the provider, nor is it possible to draw conclusions about previously visited sites. Upon user request, the stored statistical data can be reset or completely deactivated at any time.

Transmission to the Provider’s Infrastructure

In addition to encryption with the university key and any other time/location-dependent keys, each data record transferred to the provider’s infrastructure is also secured with an additional key from the provider. Thereby only indistinguishable data records are transferred and the use of a cloud provider to accept the data is possible without risk. The partial decryption of the data records by the provider is only carried out in its own infrastructure on specially secured systems. Every form of data transmission is also secured with additional transport encryption. The retention of personal scan data in the provider’s IT infrastructure is generally limited to 28 days; older contact scans are continuously deleted.

Data Storage Without Unique Identifiers

In the transferred records, there are no identifiers or otherwise consistent characteristics accessible to the operator from which a motion profile—even in anonymous form—could be derived. This is guaranteed by a consistent decoupling of registered user and location data from continuously collected scan data via encrypted links as well as by a continuous time/location-dependent re-encryption of corresponding scan data prior to each transmission. Due to a random component embedded in the encryption technology, even successive scans of individual users cannot be assigned to them.

Consent to Data Collection

The web application does not generate or collect personal data 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 is only collected with the express consent of the user during registration. With each scan process carried out by the user, a time/place limited consent to the use of personal data in case of infection is given, which can be revoked in accordance with the German Infection Protection Act with a period of notice of four weeks by using a corresponding function in the web application. In addition, the provider undertakes to continuously delete all scan data collected after 4 weeks. Data stored locally in the browser memory can be deleted at any time at the user's request using the corresponding function in the web application or by emptying the browser storage.

Data Processing

Provider

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 processed data is stored only volatilely in the main memory of the server systems and is not correlated with the encrypted user or location data. The provider undertakes to implement these measures permanently. Irrespective of this, 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 provider. 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 links is implemented via independent server systems of the provider, 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 sets, which can only be decrypted selectively in case of infection and with the cooperation of the university and the provider, no security-relevant concerns arise for the server infrastructure of the provider. Using a cloud provider based in Germany is therefore not critical for these purposes. The initial decryption of the received data sets by the provider, i.e. the generation and processing of statistical information, is performed exclusively on the provider's internal 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 initiate infection tracing. Subsequently, the provider 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 checked and confirmed by the responsible person. Using the scan keys of the affected user identified afterwards, all contact scans of persons are then found at the same time at the same place, returned and also decrypted in the browser of the responsible person. In a final step, the registration data of all contact persons identified in this way is delivered and decrypted. 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 contacting the responsible person. The responsible person also has access to checksums on the registered user and location data as well as on the PIN codes (if assigned) entered by the users during registration and scanning processes, which reliably detects misuse of the contact registration by third parties. At no time does the provider gain access to decrypted data records of any kind, but logs the time of each tracing request to prevent misuse by the university.

Health Authorities

The contact details of users directly affected by contact tracing are, by their very nature, intended to be passed on 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 sites 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 to protect uninvolved users and user stays, remain valid.

Epidemiologists

For statistical purposes, in particular to monitor the effectiveness of containment measures, and for the purpose of further research into the spread of the corona virus, completely anonymized, i.e. site-related aggregated data sets are generated without any personal reference. These data sets are used by the provider 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, patterns of spread etc. is possible without inference to individual users and thus an improvement in pandemic control.

Encryption

In the course of the initial setup, a university certificate for the encryption of user data in QRONITON is generated, 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 provider. All certificates are transmitted to the respective parties when the web application is accessed. The following steps describe the corresponding processes of the QRONITON service in the university environment.

Step 1: QR Code Generation

A unique web URL is retrieved by the provider 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 asymmetrically encrypted with the certificates and transmitted to the provider.

Step 2: User Registration

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

Step 3: Contact Scan

By scanning a QR code, the web application is launched. The location key on the device is extracted from the URL fragment, but not transferred to the web application. In addition, time keys for the QR code are retrieved from the provider for each 30-minute interval of the selected length of stay. Combining both keys results in time/location dependent composite keys that 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 provider together with the user information about the scanning process (time, duration, intensity).

Step 4: Tracing

To initiate contact tracing, a specific user key is transmitted by the user or the university. This allows the identification and decryption of all time/location dependent composite keys used by the user concerned through his or her contact scans. In turn, all other contact data records of other users protected with this key can also be decrypted. The resulting accessible user and location data of all contact persons are transmitted (still asymmetrically encrypted) to the university or authority, which decrypts them in the browser with the private key of their certificate.

Encryption Technology

Within the scope of each data collection and data processing in the QRONITON service, cryptographic primitives and encryption techniques are used as described below.

Symmetric Encryption

A randomly generated key of 128 bit length and AES-GCM, i.e. Authenticated Encryption with Associated Data (AEAD), with a nonce of 96 bit length and a Message Authentication Code (tag) of 128 bit length is used. The parameters of the encryption and its results are transmitted to the provider's infrastructure in the byte-coded format Nonce | Ciphertext | Tag.

Asymmetric Encryption

Public keys are available as X.509 certificates with 2048 bit 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, a nonce of 96 bits and a Message Authentication Code (TAG) of 128 bits are also 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. The hash algorithm SHA-256 (SHA-2) is used, for mask generation MGF1 is also used with SHA-256 (SHA-2). 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 to the infrastructure of the provider transferred. Within the scope of encryption, all recommendations of the current state of the art are implemented according to RFC6160.

Key Generation

For the generation of symmetric keys with a length of 256 bits from user data (entered or retrieved via an identity management system), the Key Derivation Function PBKDF2 with 100.000 iterations is used. A Salt is not used because of the lack of a reconstructable 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 are preferred for key exchange during connection establishment. HTTP Strict Transport Security (HSTS) with a minimum duration of two years is used for all users of the web application.