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.

In order to reliably contain further spreading of the corona virus, contact persons must be quickly identified and notified in the event of infection. This mostly paper-based process of contact recording is costly for institutions and health authorities alike and raises concerns about the protection of personal data. With QRONITON the contact recording by means of individual scanning of QR codes can be implemented effectively and at the same time the privacy of the users can be better protected.

Photo: Astrid Eckert / TUM

QRONITON was developed in cooperation with health authorities and the Robert Koch Institute and satisfies the most stringent data protection requirements. User contact data and contact chains collected via scans are encrypted multiple times and remain inaccessible to health authorities until a concrete case of infection occurs. The use of time/location-dependent encryption also ensures that only data from directly affected users with an acute risk of infection is passed on. Access to unencrypted data by the operator of the IT service is excluded at all times. In the course of an external audit of the solution, order data processing with QRONITON was classified as harmless.

QRONITON is intuitive, easy to use and platform-independent. The browser-based web solution works on standard smartphones and does not require any software installation – even users without their own mobile devices have been considered. Design and development of the service began in March 2020, and a successful field trial has been running at the Technical University of Munich since June. QRONITON was tested by numerous users, is technically mature and ready for university-wide use.

This document describes data protection compliant processes with QRONITON for an effective and secure tracing of infection chains in the university environment.

Contents

Overview of functions

With QRONITON, contacts between users are documented via joint scanning of QR codes. These contact scans can be evaluated by universities and health authorities in case of infection for the reconstruction of infection chains. Due to the consistent use of encryption, a particularly high level of security against misuse of personal data of users is achieved. At the same time, as a conventional web application, the system is easy to use for users and responsible persons and offers health authorities significant added value in the fight against pandemics due to its particularly high data quality.

Access for universities and authorities

Before the first use of the service, an authenticated system access is created for the university. During this process, a certificate is generated for the encryption of all user data in QRONITON, so that the operator does not process unencrypted data at any time. Optionally, an additional access for the responsible local health authority can be created to enable them to directly trace contacts without assistance from the university.

Processes in QRONITON

In the following all necessary procedures for the use of QRONITON in the university environment are described in detail. This includes the generation of QR codes, different variants of user registration, performing contact scans and tracing infection chains.

Generation of QR codes

The generation and use of QR Codes in QRONITON is basically permitted to every user in order to promote the widest possible distribution within the university. A direct assignment of QR codes to rooms is possible, but not mandatory. Additional information of this kind can be helpful for contact tracing, but the personal contacts and contact chains documented by scans are decisive. Accordingly, both location-bound and event-related QR codes can be generated, e.g. for courses of the current semester. Other occasions where members of the university meet, such as student council events or external activities at the university, can also be mapped in this way.

Possible uses

All QR codes in QRONITON contain an individual web address, through which users are automatically forwarded to the web application when scanned. A storage of this address in NFC tags as an alternative to scanning by camera is also possible in principle. During the generation of the QR codes, optional additional information about the place of use (e.g. office, lecture hall, seminar room, laboratory, etc.) can be specified, which, together with further user input during scans, e.g. the length of stay, is available in a later contact tracing.

Alternatively, QR codes can be generated event-related and optionally the concrete duration of the contact (e.g. 90 minutes for lectures) can be defined in advance. In both variants, capacity limits can also be specified on request, so that users are shown a warning message if rooms are overbooked. Each user also has an individual digital QR code available for retrieval in the web application, for example to voluntarily document learning groups, spontaneous meetings or other activities in small groups.

Control options

The current number of registered users can always be called up anonymously via the web addresses stored in the QR codes. In order to comply with the general documentation obligation as well as room-related capacity limits, simple control options can be realized on site – together with a record of the registration on the users' devices. The implementation of corresponding measures is the responsibility of the university.

Generating large volumes of QR codes

Via an authenticated access, i.e. by a group of people defined by the university in the Identity Management System, even large quantities of QR codes can be generated automatically. For this purpose, a CSV file with the information of the required QR codes must be created (e.g. via Excel) and imported into the web application. The underlying interface for QR code generation can also be integrated directly into the campus management system used on site and made available to employees and lecturers for rooms and events under their own responsibility. A description of the existing interfaces is provided. The realization of a corresponding connection is the responsibility of the university.

User registration

Registration of users in QRONITON is browser-based, with connection to the university's Identity Management System. Furthermore, users without a campus ID and/or their own smartphone, can also be registered for use of the service.

Registration with campus ID

During the registration process, users are directed to the Identity Management System's log-in page, in order to enter their access data here. With successful log-in, their name and internal system ID are returned to the QRONITON registration page. The user supplements this data with his/her current telephone number and the postal code of his/her place of residence.

Registration without campus ID

For users who do not have their own ID in the Identity Management System, first and last name as well as telephone number and postal code of the place of residence are queried. The rest of the registration process does not differ from that with campus ID.

Users without a smartphone

Persons without their own smartphone can also access the registration page from their PC (or from the PC of an assisting person) and create a personalized QR code to take with them as a printout. The process is similar to the two variants described at the beginning with or without campus ID.

Regardless of the respective registration variant, users in need of special security can also define a PIN code, which must be entered during each scan process and protects against misuse in the event of loss or theft of the smartphone (or the personalized QR code). Contact tracing in the event of infection detects incorrect PIN entries and reports them to the responsible operator for further verification. Access to the contact data of the person concerned remains possible.

For all variants of registration applies that personal data is collected and processed exclusively in the user's browser. After querying all required contact data, these are encrypted directly on the user's device with a university or authority certificate and are used in QRONITON exclusively in this non-readable form. Decryption takes place only in the event of infection and only on devices belonging to the responsible authorities.

Scanning QR codes

Recording contacts via scans of QR codes is simple, very flexible and requires only a few seconds to complete, even for inexperienced users.

Scan application

Scanning QR codes requires a mobile device with a camera and an installed browser, which is the case for virtually all available smartphones. Internet connectivity via the mobile phone network or the university's own WLAN network is also required. There are no further requirements for the use of QRONITON. The web application is operational on all operating systems (Android, iOS, Windows Phone etc.) and independent of their version status.

A QR code can be scanned directly from the browser, i.e. by manually opening the web application and authorizing the camera. Alternatively, third-party QR scan apps or, on newer devices, the camera app of the manufacturer or operating system can be used directly. In all cases, the user is redirected to the QR code specific web page for contact registration immediately after the scan. If the user is not yet registered for QRONITON, the corresponding registration page is displayed.

In principle, the web address stored in the QR codes can also be transmitted to individual users or user groups via other channels, e.g. NFC tags have already been successfully tested in door signs for wireless transmission when touched. Distribution via e-mail for pre-booking at larger events is also conceivable in principle.

Recorded information

After calling up the registration page of a QR code, several pieces of information are requested to increase the data quality and thus facilitate later contact tracing. First of all, the intensity of the contact must be specified, e.g. with/without distance and/or mask, lecture/group work/individual conversation* or similar. If the QR code does not already contain an explicit duration of the event, the expected duration of the stay is requested from the user using quick suggestions, e.g. short contact as well as 45/60/90/120 minutes of stay*. A check-in and check-out mechanism is also available in the application. If specified by the user during registration, the user's PIN code must also be entered at this point.

Processing of contact scans

After entering all the necessary information, a record of the scanned QR code is generated on the user's device, which can also be called up later via the web application until the next scan. In addition, warnings are issued in case of overcrowding in rooms with limited capacity, and anonymous scan and contact statistics are updated locally on the user's device for their personal use.

**The options relevant to the university are determined system-wide during the set-up.*

Users without a smartphone

Users without a smartphone carry their personalized QR code generated during registration. They ask the event organizer (or any other QRONITON user) to scan this QR Code. The web application now expects the scan of another QR code, i.e. the one of the room or event, to perform the contact registration. All further steps are identical to those of smartphone users. The personal data of the assisting person remains unaffected by this process (although a direct link between the two persons remains possible).

Contact tracing

In the event of an infection, the health authority contacts the newly infected person and establishes his or her affiliation to the university or his/her stay there. If the authority has its own QRONITON access, it triggers the contact tracing with the help of the person concerned. If this is not possible, the university is informed and requested to start the contact tracing process.

Variant 1: Contact tracing with authority's access

The health authority generates a six-digit authorization code via its QRONITON access and asks the person concerned to enter this code into his/her browser. Contact tracing in QRONITON then starts and can be monitored directly via the authority access. If this does not happen, e.g. because the person concerned does not comply with the request, the health authority contacts the university (see variant 2).

Variant 2: Contact tracing without authority's access

The health authority informs the university of the personal data and contact details of the person concerned and requests that contact be traced. The university identifies the student in the Identity Management System and enters his or her campus ID into their QRONITON access, which starts the contact tracing. For infected guests, service providers or other persons without their own campus ID, contact tracing can also be triggered by entering their telephone number and postal code. The cooperation of affected persons is not necessary.

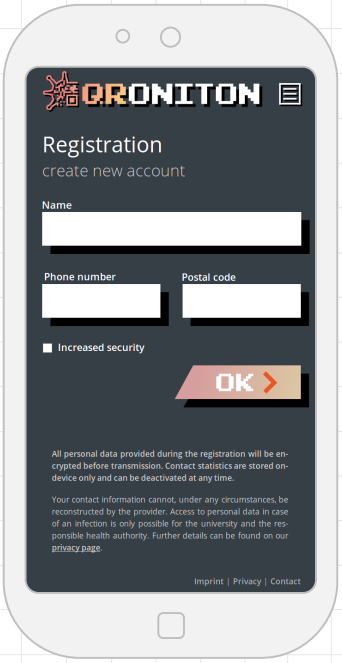
Reconstruction of contact chains

After triggering the tracing in QRONITON, all direct contact persons are identified, i.e. all those persons who were at the same place at the same time and scanned QR Codes together with the person concerned. Stays of persons at other locations, i.e. scans of QR Codes not affected, remain inaccessible. The resulting contact details are transmitted to the end device of the tracing authority, i.e. to the browser of an authenticated university or public authority employee, where it is decrypted using the certificate generated during the setup. These contact details are not visible to the operator.

The tracing results can be viewed sorted by location/event, time, duration and intensity of the individual contacts. When using PIN codes, incorrect entries are highlighted for further verification. Together with the contact details of the persons concerned, the collected data points can be exported as CSV file for further processing.

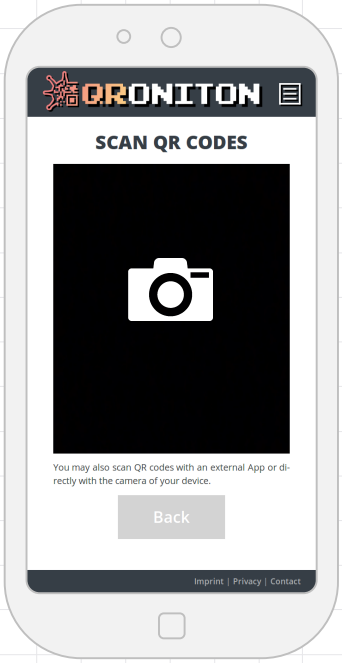
Process from the user's perspective

The use of the QRONITON application in the browser is intuitive and modeled on modern smartphone apps. Due to a transparent mode of operation with guided use, there is clarity at any time about the next steps and collected information. The web application is independent of the operating system and does not require any software installation.



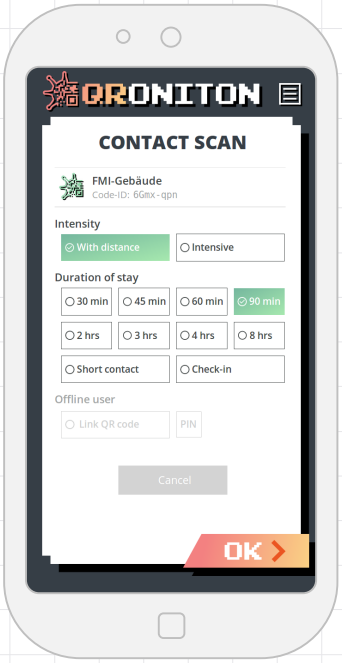
Registration process

Entering campus ID, telephone number and postal code



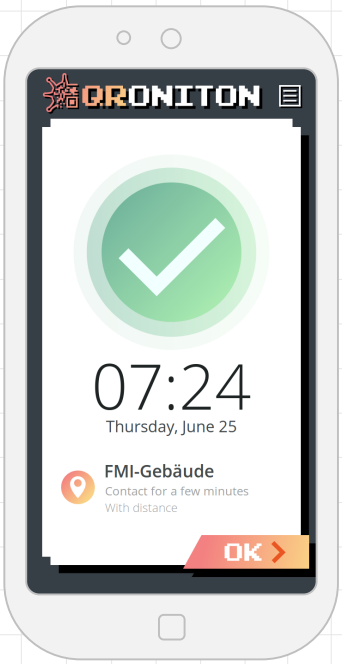
Scanning QR codes

Camera access in the browser or via an external scan app



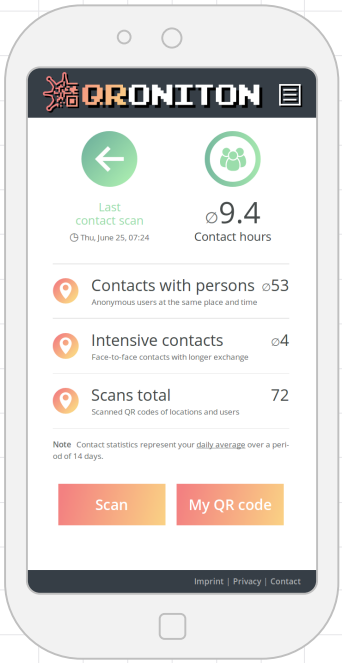
Recorded information

Contact location, time, duration, and intensity



Recording evidence

Access to the last scanned QR code for room checks



Anonymous contact statistics

Functional evidence and learning effect for risk minimization

Personal QR code

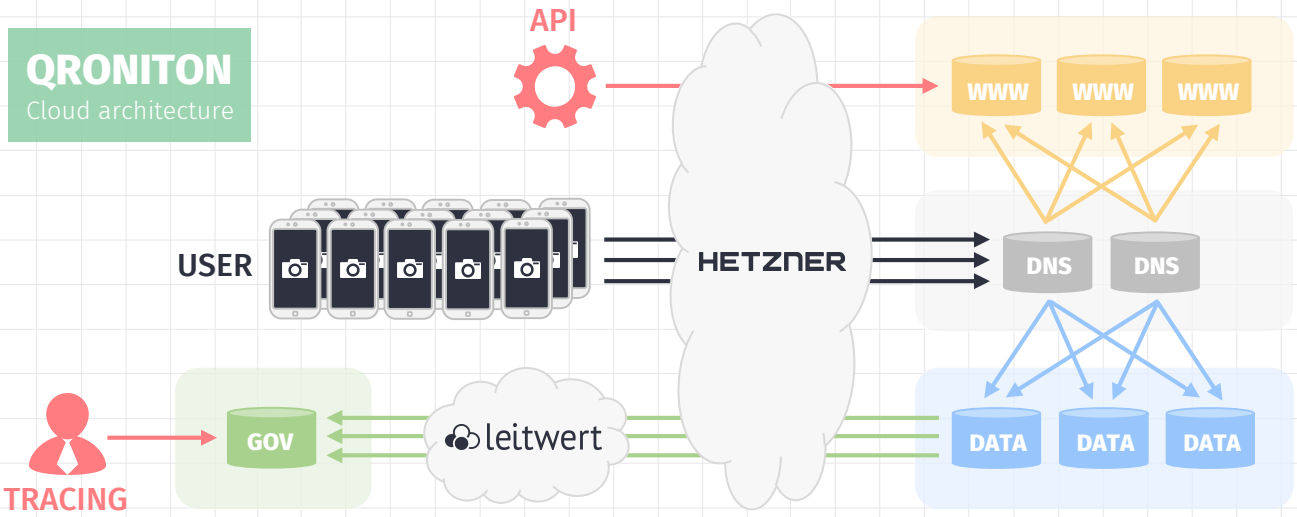
Display of a digital QR code for spontaneous contacts

Set-up of the IT infrastructure

In the IT infrastructure of the QRONITON service, numerous server systems are used in two different network environments for performance and security reasons. All systems are operated exclusively in Germany, in a cloud environment of the hosting provider *Hetzner* and in the data center of the operator *Leitwert* in Frankfurt. The infrastructure is highly scalable and designed for a seven-digit number of users and QR codes.

Overview of the architecture

The following diagram shows all systems and dependencies in the QRONITON infrastructure. If necessary, individual (or all) sub-components can be operated in the university's own data center. In this case, monitoring, maintenance and support is the responsibility of the university.



API access

QR codes can be generated automatically via a REST-based interface. In addition, current scan statistics as well as results of individual contact tracing can be retrieved. Authentication is carried out via the certificate of the university generated during the setup. An interface description is available on request.

Data storage

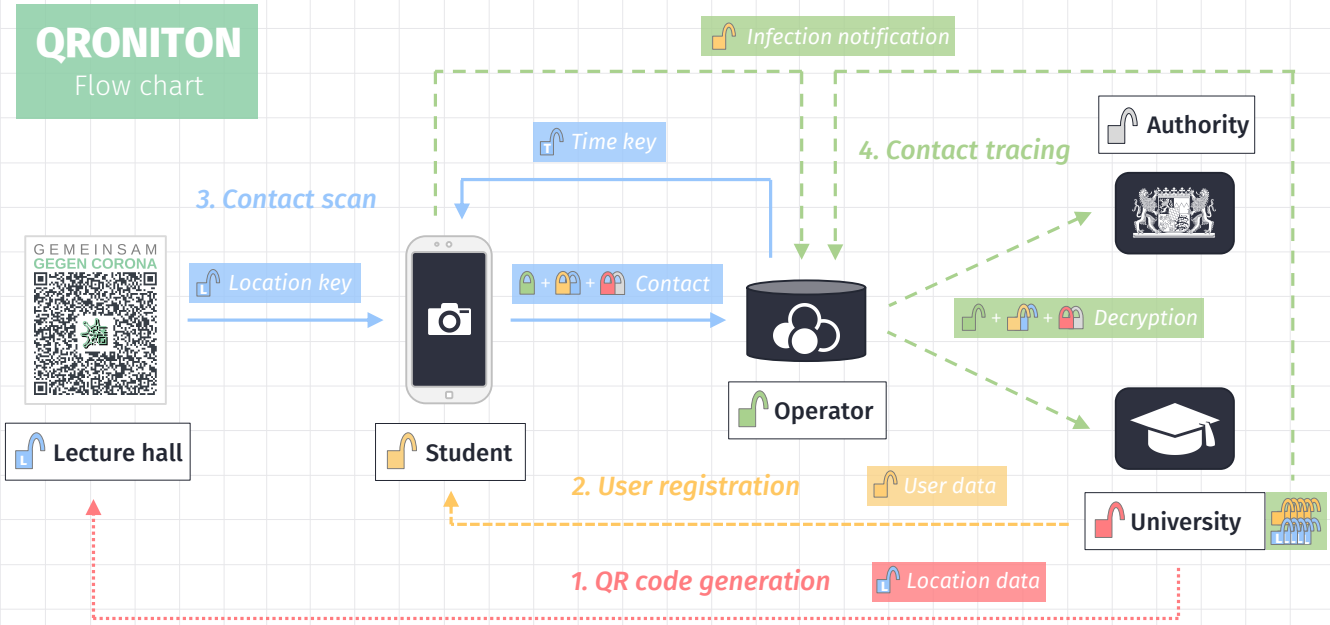
The data records, which are always encrypted multiple times, are stored on the cloud systems provided for this purpose and periodically sent to the operator's infrastructure. There, a first partial decryption and storage in an NoSQL database (MongoDB) takes place. Each data record is automatically and irrevocably deleted four weeks after it has been collected.

Implementation

All systems in the infrastructure are operated under the Ubuntu Server operating system. The web frontend was implemented in JavaScript (ECMAv6) and CSS3, backend processes in PyPy7 with uWSGI connection to the web server lighttpd. The source code of the web application was deliberately not minimized or obfuscated and can be viewed by everyone directly in the browser.

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 address
Donaustrasse 17
85049 Ingolstadt
GERMANY

GEMEINSAM
GEGEN CORONA

https://qroniton.eu