QRONITON

Sichere Kontaktnachverfolgung mit QR-Codes

QRONITON ist ein Contact-Tracing-Dienst, mit dem Einrichtungen ihrer Dokumentationspflicht in der Pandemiebekämpfung nachkommen und Gesundheitsämter schnell gefährdete Personen auffinden können. Die Browser-basierte Web-Lösung funktioniert mit QR-Codes, vereinfacht die Kontaktnachverfolgung und schützt persönliche Daten der Nutzer gegen Missbrauch.

Um eine weitere Ausbreitung des Corona-Virus zuverlässig einzudämmen, müssen im Infektionsfall Kontaktpersonen schnell identifiziert und benachrichtigt werden. Dieser zumeist papiergebundene Prozess der Kontakterfassung ist für Einrichtungen und Gesundheitsbehörden gleichermaßen aufwendig und zieht Bedenken hinsichtlich des Schutzes persönlicher Daten nach sich. Durch QRONITON lässt sich die Kontakterfassung mittels individuellem Scannen von QR-Codes wirkungsvoll umsetzen und gleichzeitig die Privatsphäre der Nutzer besser schützen.

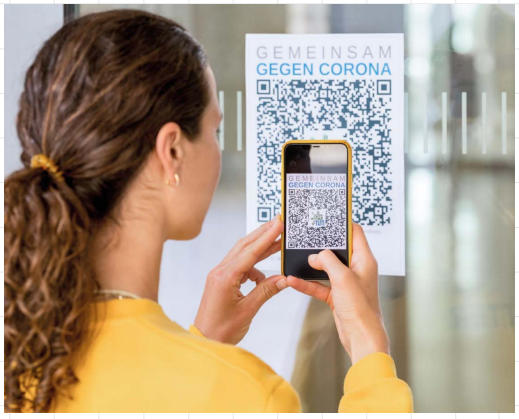


Bild: Astrid Eckert / TUM

QRONITON wurde im Austausch mit Gesundheitsbehörden und dem Robert Koch Institut entwickelt und genügt höchsten Datenschutzanforderungen. Kontaktdaten der Nutzer sowie über Scans erfasste Kontaktketten werden mehrfach verschlüsselt und bleiben bis zu einem konkreten Infektionsfall für Gesundheitsbehörden unzugänglich. Durch den Einsatz einer Zeit/Orts-abhängigen Verschlüsselung wird zudem sichergestellt, dass ausschließlich Daten von direkt betroffenen Nutzern mit akutem Infektionsrisiko weitergegeben werden. Ein Zugriff auf unverschlüsselte Daten durch den Betreiber des IT-Dienstes ist zu jedem Zeitpunkt ausgeschlossen. Im Zuge einer externen Prüfung der Lösung wurde eine Auftragsdatenverarbeitung mit QRONITON als unbedenklich eingestuft.

QRONITON ist intuitiv, einfach zu bedienen und plattformunabhängig. Die Browser-basierte Web-Lösung funktioniert auf handelsüblichen Smartphones und erfordert keine Installation von Software – auch an Nutzer ohne eigene Mobilgeräte wurde gedacht. Konzeption und Entwicklung des Dienstes begannen bereits im März 2020, seit Juni läuft ein erfolgreicher Feldversuch an der Technischen Universität München. QRONITON wurde von zahlreichen Nutzern erprobt, ist technisch ausgereift und steht für einen hochschulweiten Einsatz bereit.

Mit diesem Dokument werden datenschutzkonforme Abläufe mit QRONITON für eine effektive und sichere Nachverfolgung von Infektionsketten im Hochschulumfeld beschrieben.

Inhaltsverzeichnis

Funktionsüberblick

Mit QRONITON werden Kontakte zwischen Nutzern über gemeinsames Scannen von QR-Codes dokumentiert. Diese Kontakt-Scans können von Hochschulen und Gesundheitsbehörden im Infektionsfall zur Rekonstruktion von Infektionsketten ausgewertet werden. Aufgrund des durchgängigen Einsatzes von Verschlüsselung wird ein besonders hohes Maß an Sicherheit gegenüber einem Missbrauch von persönlichen Daten der Nutzer erzielt. Gleichzeitig ist das System als herkömmliche Web-Anwendung für Nutzer und Verantwortliche leicht zu bedienen und bietet Gesundheitsbehörden aufgrund einer besonders hohen Datenqualität einen signifikanten Mehrwert in der Pandemiebekämpfung.

Hochschul- und Behördenzugang

Vor Ersteinsatz des Dienstes wird für die Hochschule ein authentifizierter Systemzugang angelegt. Im Rahmen dieses Prozesses wird ein Zertifikat für die Verschlüsselung aller Nutzerdaten in QRONITON erzeugt, so dass der Betreiber zu keinem Zeitpunkt unverschlüsselte Daten verarbeitet. Optional kann auch ein weiterer Zugang für die zuständige Gesundheitsbehörde vor Ort angelegt werden, um dieser eine direkte Kontaktnachverfolgung ohne Hilfestellung durch die Hochschule zu ermöglichen.

Abläufe in QRONITON

Im Folgenden werden alle nötigen Abläufe für die Verwendung von QRONITON im Hochschulumfeld näher beschrieben. Dies umfasst die Erzeugung von QR-Codes, verschiedene Varianten der Nutzerregistrierung, die Durchführung von Kontakt-Scans sowie die Nachverfolgung von Infektionsketten.

Erzeugung von QR-Codes

Die Erzeugung und Verwendung von QR-Codes in QRONITON ist grundsätzlich jedem Nutzer gestattet, um eine möglichst große Verbreitung innerhalb der Hochschule zu fördern. Eine direkte Zuordnung von QR-Codes zu Räumen ist möglich, aber nicht zwingend erforderlich. Zusatzinformationen dieser Art können für die Kontaktnachverfolgung durchaus hilfreich sein, entscheidend sind aber die über Scans dokumentierten Personenkontakte und Kontaktketten. Dementsprechend lassen sich sowohl ortsgebundene als auch veranstaltungsbezogene QR-Codes erzeugen, bspw. für Lehrveranstaltungen des aktuellen Semesters. Auch andere Anlässe, bei denen Hochschulangehörige zusammentreffen, wie Fachschaftsveranstaltungen oder externe Aktivitäten an der Hochschule, lassen sich so abbilden.

Nutzungsmöglichkeiten

Alle QR-Codes in QRONITON beinhalten eine individuelle Web-Adresse, worüber Nutzer bei Scans automatisch zur Web-Anwendung weitergeleitet werden. Eine Hinterlegung dieser Adresse in NFC-Tags als Alternative zum Scannen per Kamera ist prinzipiell ebenso möglich. Während der Erzeugung der QR-Codes können optionale Zusatzinformationen über den Verwendungsort (z.B. Büro, Hörsaal, Seminarraum, Labor etc.) angegeben werden, die zusammen mit weiteren Nutzereingaben bei Scans, bspw. der Aufenthaltsdauer, in einer späteren Kontaktnachverfolgung zur Verfügung stehen.

Alternativ dazu können QR-Codes veranstaltungsbezogen erzeugt und optional auch die konkrete Dauer des Kontakts (z.B. 90 Minuten bei Vorlesungen) vorab festgelegt werden. In beiden Varianten können auf Wunsch auch Kapazitätslimits angegeben werden, so dass Nutzern bei Überbelegung von Räumen eine Warnmeldung angezeigt wird. Jedem Nutzer steht darüber hinaus auch ein individueller digitaler QR-Code zum Abruf in der Web-Anwendung zur Verfügung, bspw. um Lerngruppen, spontane Zusammenkünfte oder andere Aktivitäten in Kleingruppen freiwillig zu dokumentieren.

Kontrollmöglichkeiten

Über die in den QR-Codes hinterlegten Web-Adressen kann stets die aktuelle Zahl der eingebuchten Nutzer in anonymer Form abgerufen werden. Für die Einhaltung der generellen Dokumentationspflicht sowie raumbezogener Kapazitätsgrenzen lassen sich – zusammen mit einem Erfassungsnachweis auf den Geräten der Nutzer – damit prinzipiell auch einfache Kontrollmöglichkeiten vor Ort realisieren. Die Umsetzung entsprechender Maßnahmen obliegt der Hochschule.

Erzeugung großer QR-Code-Mengen

Über einen authentifizierten Zugang, d.h. durch einen von der Hochschule im Identity-Management-System festgelegten Personenkreis, lassen sich auch große Mengen von QR-Codes in automatisierter Weise erzeugen. Hierfür ist eine CSV-Datei mit den Informationen der benötigten QR-Codes (z.B. über Excel) anzulegen und in die Web-Anwendung zu importieren. Die zugrunde liegende Schnittstelle zur QR-Code-Erzeugung kann prinzipiell auch direkt in das vor Ort eingesetzte Campus-Management-System integriert und darüber Mitarbeitern und Dozenten für Räume und Veranstaltungen in eigener Verantwortlichkeit zugänglich gemacht werden. Eine Beschreibung der vorhandenen Schnittstellen wird bereitgestellt, die Realisierung einer entsprechenden Anbindung obliegt der Hochschule.

Registrierung von Nutzern

Die Registrierung von Nutzern in QRONITON erfolgt Browser-basiert mit Anbindung an das Identity-Management-System der Hochschule. Darüber hinaus können auch Nutzer ohne Campus-Kennung und/oder eigenes Smartphone für die Nutzung des Dienstes registriert werden.

Registrierung mit Campus-Kennung

Während des Registrierungsprozesses wird der Nutzer auf die Login-Seite des Identity-Management-Systems weitergeleitet, um dort seine Zugangsdaten einzugeben. Bei erfolgreichem Login wird dessen Name und interne System-ID an die Registrierungsseite von QRONITON zurückgeliefert. Der Nutzer ergänzt diese Daten um seine aktuelle Telefonnummer sowie die Postleitzahl seines Wohnortes.

Registrierung ohne Campus-Kennung

Für Nutzer ohne eigene Kennung im Identity-Management-System werden Vor- und Nachname sowie Telefonnummer und Postleitzahl des Wohnortes abgefragt. Der weitere Verlauf der Registrierung unterscheidet sich nicht von demjenigen mit Campus-Kennung.

Nutzer ohne Smartphone

Personen ohne eigenes Smartphone können die Registrierungsseite auch über ihren PC (bzw. über den PC einer Hilfsperson) aufrufen und sich darüber einen personalisierten QR-Code zur Mitführung als Ausdruck erstellen. Der Registrierungsprozess gleicht im weiteren Verlauf den beiden eingangs beschriebenen Varianten mit bzw. ohne Campus-Kennung.

Unabhängig von der jeweiligen Registrierungsvariante kann von besonders sicherheitsbedürftigen Nutzern auch ein PIN-Code festgelegt werden, der bei jedem Scan-Vorgang anzugeben ist und gegen Missbrauch bei Verlust oder Diebstahl des Smartphones (bzw. des personalisierten QR-Codes) schützt. Mit einer Kontaktnachverfolgung im Infektionsfall werden inkorrekte PIN-Eingaben erkannt und dem verantwortlichen Bearbeiter zur weiteren Prüfung gemeldet. Der Zugriff auf die Kontaktdaten des Betroffenen bleibt dabei weiterhin möglich.

Für alle Varianten der Registrierung gilt, dass personenbezogene Daten ausschließlich im Browser des Nutzers erhoben und verarbeitet werden. Nach Abfrage aller benötigten Kontaktdaten werden diese unmittelbar auf dem Gerät des Nutzers mit einem Hochschul- bzw. Behördenzertifikat verschlüsselt und in QRONITON ausschließlich in dieser nicht-lesbaren Form weiterverwendet. Eine Entschlüsselung erfolgt nur im Infektionsfall und nur auf Geräten der verantwortlichen Stellen.

Scannen von QR-Codes

Die Erfassung von Kontakten über Scans von QR-Codes ist einfach, sehr flexibel und erfordert auch für unerfahrene Nutzer nur wenige Sekunden in der Durchführung.

Scan-Anwendung

Für das Scannen von QR-Codes wird ein Mobilfunkgerät mit Kamera und installiertem Browser benötigt, was für praktisch alle erhältlichen Smartphones zutrifft. Zudem ist Internet-Konnektivität über das Mobilfunknetz oder das hochschuleigene WLAN-Netz notwendig. Weitere Anforderungen für die Verwendung von QRONITON bestehen nicht, die Web-Anwendung ist insbesondere auf allen Betriebssystemen (Android, iOS, Windows Phone etc.) und unabhängig von deren Versionsstand lauffähig.

Das Scannen eines QR-Codes kann direkt aus dem Browser heraus erfolgen, d.h. durch vorherigen manuellen Aufruf der Web-Anwendung und Freigabe der Kamera. Alternativ dazu können auch QR-Scan-Apps von Drittanbietern oder auf neueren Geräten auch direkt die Kamera-App des Herstellers bzw. Betriebssystems verwendet werden. In allen Fällen wird der Nutzer unmittelbar nach dem Scan auf die QR-Code-spezifische Web-Seite zur Kontakterfassung weitergeleitet. Ist der Nutzer noch nicht für QRONITON registriert, wird die entsprechende Registrierungsseite vorangeschaltet.

Prinzipiell lässt sich die in den QR-Codes hinterlegte Web-Adresse einzelnen Nutzern oder Nutzergruppen auch über andere Kanäle übermitteln, bspw. wurden bereits NFC-Tags in Türschildern zur drahtlosen Übertragung bei Berührung erfolgreich erprobt. Auch eine Verteilung via E-Mail zur Vorabeinbuchung bei größeren Veranstaltungen ist grundsätzlich denkbar.

Erfasste Informationen

Nach Aufruf der Erfassungsseite eines QR-Codes werden mehrere Informationen zur Erhöhung der Datenqualität und damit zur Erleichterung einer späteren Kontaktnachverfolgung abgefragt. Zunächst ist die Intensität des Kontakts anzugeben, bspw. mit/ohne Abstand und/oder Maske, Vorlesung/Gruppenarbeit/Einzelgespräch* oder ähnliches. Sofern im QR-Code nicht bereits eine explizite Dauer der Veranstaltung hinterlegt ist, wird die erwartete Aufenthaltszeit vom Nutzer anhand von Schnellvorschlägen abgefragt, bspw. Kurzkontakt sowie 45/60/90/120 Minuten Aufenthalt*. Ein Checkin- und Checkout-Mechanismus ist ebenfalls in der Anwendung vorhanden. Falls vom Nutzer im Zuge der Registrierung festgelegt, muss an dieser Stelle auch dessen PIN-Code mit angegeben werden.

Verarbeitung der Kontakt-Scans

Nach Eingabe aller benötigten Informationen wird auf dem Gerät des Nutzers ein Erfassungsnachweis für den gescannten QR-Code generiert, der bis zum nächsten Scan auch zu einem späteren Zeitpunkt über die Web-Anwendung abgerufen werden kann. Ferner werden Warnhinweise bei Überbelegung kapazitätsbeschränkter Räume ausgegeben sowie anonyme Scan- und Kontaktstatistiken lokal auf dem Gerät des Nutzers für dessen persönliche Verwendung aktualisiert.

**Die für die Hochschule relevanten Auswahlmöglichkeiten werden im Rahmen der Einrichtung systemweit festgesetzt.*

Nutzer ohne Smartphone

Nutzer ohne Smartphone führen ihren bei der Registrierung erzeugten personalisierten QR-Code mit sich. Sie bitten den Veranstaltungsleiter (oder einen beliebigen anderen QRONITON-Nutzer), diesen QR-Code zu scannen. Die Web-Anwendung erwartet nun den Scan eines weiteren QR-Codes, d.h. den des Raumes oder der Veranstaltung, um die Kontakterfassung durchzuführen. Alle weiteren Schritte gleichen denen von Smartphone-Nutzern. Die persönlichen Daten der Hilfsperson bleiben bei diesem Vorgang unberührt (wenngleich auch eine direkte Verknüpfung beider Personen möglich bleibt).

Kontaktnachverfolgung

Im Infektionsfall tritt die Gesundheitsbehörde in Kontakt zur neu infizierten Person und stellt deren Zugehörigkeit zur Hochschule bzw. Aufenthalt in dieser fest. Verfügt die Behörde über einen eigenen QRONITON-Zugang, so löst sie die Kontaktverfolgung unter Mithilfe des Betroffenen selbst aus. Ist dies nicht möglich, wird die Hochschule benachrichtigt und zur Kontaktnachverfolgung aufgefordert.

Variante 1: Nachverfolgung mit Behördenzugang

Die Gesundheitsbehörde erzeugt über ihren QRONITON-Zugang einen sechsstelligen Autorisierungs-Code und fordert den Betroffenen zur Eingabe dieses Codes in dessen Browser auf. Daraufhin wird die Kontaktnachverfolgung in QRONITON gestartet und kann über den Behördenzugang unmittelbar eingesehen werden. Geschieht dies nicht, bspw. weil der Betroffene der Aufforderung nicht nachkommt, tritt die Gesundheitsbehörde mit der Hochschule in Kontakt (siehe Variante 2).

Variante 2: Nachverfolgung ohne Behördenzugang

Die Gesundheitsbehörde teilt der Hochschule Personalien und Kontaktdaten des Betroffenen mit und fordert zur Kontaktnachverfolgung auf. Die Hochschule identifiziert den Studenten im Identity-Management-System und trägt dessen Campus-Kennung in ihren QRONITON-Zugang ein, wodurch die Kontaktnachverfolgung gestartet wird. Für infizierte Gäste, Dienstleister oder andere Personen ohne eigene Campus-Kennung kann die Kontaktnachverfolgung auch unter Angabe deren Telefonnummer und Postleitzahl ausgelöst werden. Eine Mitwirkung von Betroffenen ist nicht erforderlich.

Rekonstruktion von Kontaktketten

Nach Auslösen der Nachverfolgung in QRONITON werden alle direkten Kontaktpersonen identifiziert, d.h. all diejenigen Personen, die sich zur selben Zeit am selben Ort aufgehalten und gemeinsam mit dem Betroffenen QR-Codes gescannt haben. Aufenthalte von Personen an anderen Orten, d.h. Scans von nicht betroffenen QR-Codes, bleiben unzugänglich. Die resultierenden Kontaktdaten werden an das Endgerät der nachverfolgenden Stelle, d.h. an den Browser eines authentifizierten Hochschul- oder Behördenmitarbeiters übertragen und dort unter Verwendung des bei der Einrichtung erzeugten Zertifikats entschlüsselt. Für den Betreiber sind diese Kontaktdaten nicht einsehbar.

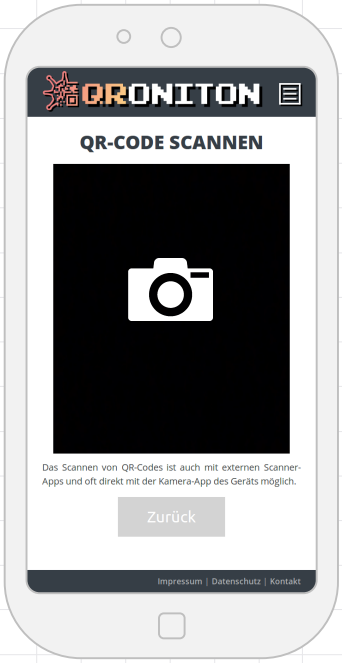
Die Ergebnisse der Nachverfolgung können sortiert nach Ort/Veranstaltung, Zeitpunkt, Dauer und Intensität der einzelnen Kontakte betrachtet werden. Bei Verwendung von PIN-Codes werden Fehleingaben zur weiteren Prüfung hervorgehoben. Zusammen mit den Kontaktdaten der Betroffenen können die erhobenen Datenpunkte zur Weiterverarbeitung als CSV-Datei exportiert werden.

Ablauf aus Sicht des Nutzers

Die Verwendung der QRONITON-Anwendung im Browser ist intuitiv und der Darstellungsart moderner Smartphone-Apps nachempfunden. Durch eine transparente Funktionsweise mit geführter Nutzung herrscht zu jedem Zeitpunkt Klarheit über die nächsten Schritte und erfassten Informationen. Die Web-Anwendung ist Betriebssystem-unabhängig und erfordert keine Installation von Software.

Registrierungsvorgang

Eingabe der Campus-Kennung, Telefonnummer und Postleitzahl



Scannen von QR-Codes

Kamerazugriff im Browser oder über externe Scan-App

Erfasste Informationen

Ort, Zeitpunkt, Dauer und Intensität des Kontakts

Erfassungsnachweis

Aufruf des zuletzt gescannten QR-Codes bei Raumkontrollen

Anonyme Kontaktstatistik

Funktionsnachweis und Lern-effekt zur Risikominimierung

Eigener QR-Code

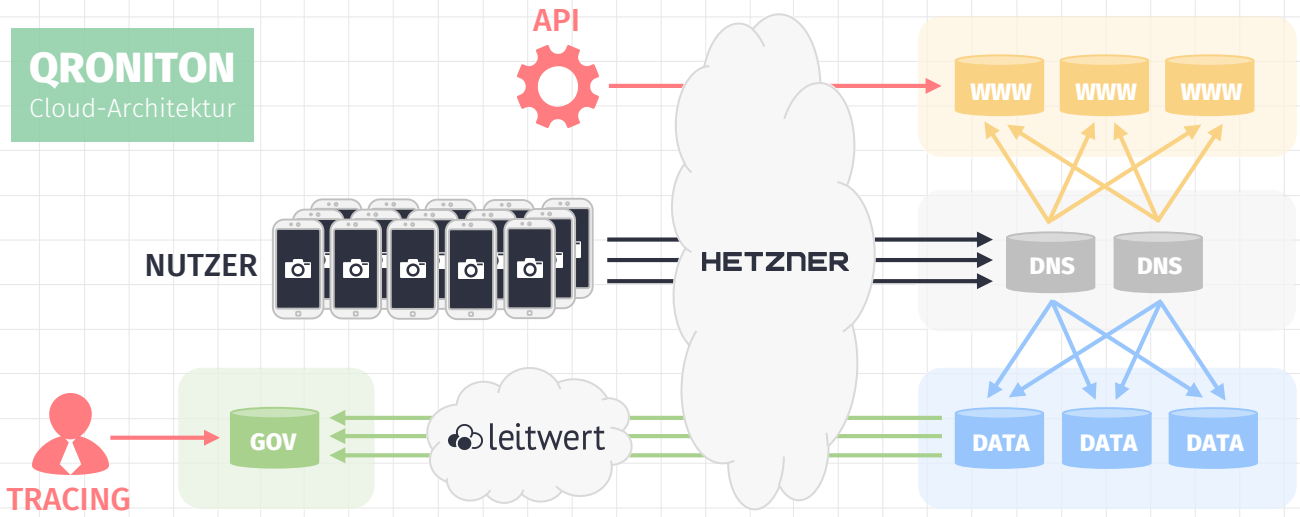
Darstellung eines digitalen QR-Codes für spontane Kontakte

Aufbau der IT-Infrastruktur

In der IT-Infrastruktur des QRONITON-Dienstes werden aus Performanz- und Sicherheitsgründen zahlreiche Server-Systeme in zwei verschiedenen Netzumgebungen eingesetzt. Alle Systeme werden ausschließlich in Deutschland betrieben, und zwar in einer Cloud-Umgebung des Hosting-Anbieters *Hetzner* sowie im Rechenzentrum des Betreibers *Leitwert* in Frankfurt. Die aufgebaute Infrastruktur ist hochgradig skalierbar und für eine siebenstellige Zahl an Nutzern und QR-Codes ausgelegt.

Architekturübersicht

Das folgende Diagramm stellt alle Systeme und Abhängigkeiten in der QRONITON-Infrastruktur dar. Falls erforderlich können einzelne (oder auch alle) Teilkomponenten im hochschuleigenen Rechenzentrum betrieben werden. Überwachung, Wartung und Pflege obliegt in diesem Fall der Hochschule.



API-Zugang

Über eine REST-basierte Schnittstelle können automatisiert QR-Codes erzeugt werden. Zudem lassen sich hierüber aktuelle Scan-Statistiken sowie Ergebnisse einzelner Kontaktnachverfolgungen abrufen. Die Authentifizierung erfolgt über das bei der Einrichtung erzeugte Zertifikat der Hochschule. Eine Schnittstellenbeschreibung wird auf Anfrage bereitgestellt.

Datenvorhaltung

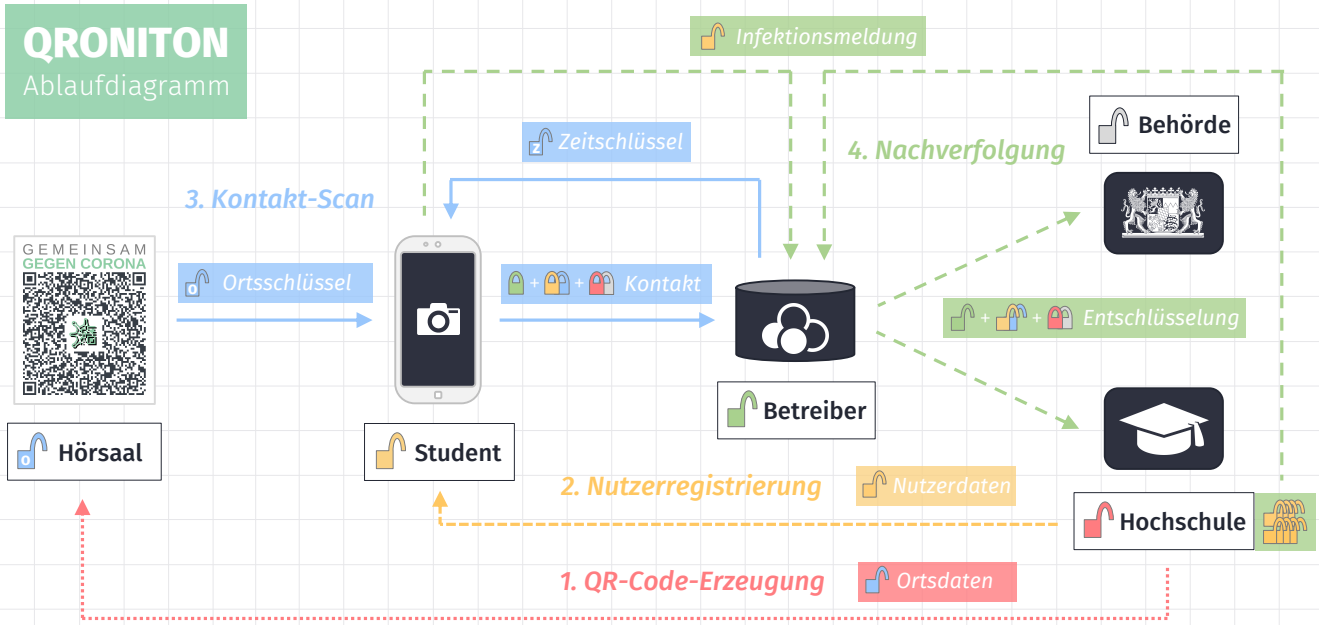
Die stets mehrfach verschlüsselten Datensätze werden auf den dafür vorgesehenen Cloud-Systemen abgelegt und periodisch an die Infrastruktur des Betreibers übertragen. Dort erfolgt eine erste Teilentschlüsselung und Ablage in einer NoSQL-Datenbank (MongoDB). Jeder Datensatz wird automatisch vier Wochen nach dessen Erhebung unwiderruflich gelöscht.

Implementierung

Alle Systeme der Infrastruktur werden unter dem Betriebssystem Ubuntu Server betrieben. Das Web-Frontend wurde in JavaScript (ECMAv6) und CSS3 implementiert, Backend-Prozesse in PyPy7 mit uWSGI-Anbindung an den Web-Server lighttpd. Der Quellcode der Web-Anwendung wurde bewusst nicht minimiert bzw. obfuskiert und ist für jedermann direkt im Browser einsehbar.

Verschlüsselungskonzept

Im Zuge der Ersteinrichtung wird ein Hochschulzertifikat [🔒] für die Verschlüsselung von Nutzerdaten in QRONITON erzeugt, optional ergänzt um einen weiteren Systemzugang für die vor Ort zuständige Gesundheitsbehörde [🔒]. Jegliche Übertragung von Daten an die QRONITON-Infrastruktur wird stets auch mit einem Zertifikat des Betreibers [🔒] gegen Datendiebstahl und Manipulation gesichert. Alle Zertifikate werden bei Aufruf der Web-Anwendung an die jeweiligen Akteure ausgeliefert. Das nachfolgende Diagramme zeigt die zugehörigen Abläufe des QRONITON-Dienstes im Hochschulumfeld.



Schritt 1: QR-Code-Erzeugung

Vom Betreiber wird eine eindeutige Web-URL zur Einbettung in den QR-Code abgerufen. Im Browser werden vom Verantwortlichen Ortsdaten zur Beschreibung der Veranstaltung bzw. des Raumes eingegeben, ein zufälliger Ortsschlüssel [🔒] generiert und als URL-Fragment (#) angehängt. Die Ortsdaten werden mit den Zertifikaten asymmetrisch verschlüsselt [🔒] und an den Betreiber übertragen.

Schritt 2: Nutzerregistrierung

Aus von der Hochschule abgerufenen (oder manuell eingegebenen) Nutzerdaten wird im Browser des Nutzers ein Nutzerschlüssel [🔒] generiert und lokal im Browser Storage abgelegt. Die Nutzerdaten werden mit den Zertifikaten asymmetrisch verschlüsselt [🔒] und an den Betreiber übertragen.

Schritt 3: Kontakt-Scan

Durch Scannen eines QR-Codes wird die Web-Anwendung aufgerufen. Aus dem URL-Fragment wird der Ortsschlüssel [🔒] auf dem Gerät extrahiert, aber nicht an die Web-Anwendung übertragen. Zudem werden für jedes 15-Minuten-Intervall der gewählten Aufenthaltsdauer Zeitschlüssel [🔒] für den QR-Code vom Betreiber abgerufen. Durch Kombination beider Schlüssel entstehen Zeit/Ort-abhängige Kompositschlüssel [🔒], die für alle zeitgleichen Kontakt-Scans eines spezifischen QR-Codes identisch sind. Mit diesen Kompositschlüsseln werden Referenzen auf die registrierten Nutzer- und Ortsdaten symmetrisch verschlüsselt, auch die Kompositschlüssel selbst werden mit dem Nutzerschlüssel [🔒] symmetrisch verschlüsselt. Alle verschlüsselten Datenpunkte werden zusammen mit den Nutzeranagaben zum Scan-Vorgang (Zeitpunkt, Dauer, Intensität) an den Betreiber übertragen.

Schritt 4: Nachverfolgung

Für das Auslösen der Kontaktnachverfolgung wird vom Nutzer oder von der Hochschule ein konkreter Nutzerschlüssel [🔓] übermittelt. Dadurch lassen sich alle Zeit/Ort-abhängigen Kompositschlüssel [🔓] identifizieren und entschlüsseln, die vom betroffenen Nutzer durch dessen Kontakt-Scans verwendet wurden. Hierüber wiederum können auch alle weiteren mit diesem Schlüssel geschützten Kontakt-Datensätze anderer Nutzer entschlüsselt werden. Die dadurch zugänglichen Nutzer- und Ortsdaten aller Kontaktpersonen werden (noch asymmetrisch verschlüsselt) an die Hochschule oder Behörde übermittelt, die diese mit dem privaten Schlüssel ihres Zertifikats [🔒 | 🔓] im Browser entschlüsseln.

Verschlüsselungstechnik (Anhang)

Im Rahmen jeder Datenerhebung und Datenverarbeitung im QRONITON-Dienst kommen die nachfolgend beschriebenen Krypto-Primitive und Verschlüsselungstechniken zum Einsatz.

Symmetrische Verschlüsselung

Es wird ein zufallsgenerierter Schlüssel der Länge 256 Bit und AES-GCM, d.h. Authenticated Encryption with Associated Data (AEAD), mit einer Nonce der Länge 96 Bit und einem Message Authentication Code (Tag) der Länge 128 Bit eingesetzt. Die Parameter der Verschlüsselung sowie dessen Ergebnisse werden Byte-kodiert im Format Nonce|Ciphertext|Tag an die Infrastruktur des Betreibers übertragen.

Asymmetrische Verschlüsselung

Öffentliche Schlüssel liegen als X.509-Zertifikate mit 2048 Bit Schlüssellänge vor. Alle damit zu verschlüsselnden Daten werden zunächst mit einem pseudo-zufällig erzeugten Schlüssel symmetrisch verschlüsselt, hierbei wird AES-GCM, d.h. Authenticated Encryption with Associated Data (AEAD), eingesetzt. Die Schlüssellänge beträgt 128 Bit, zudem wird eine Nonce der Länge 96 Bit und ein Message Authentication Code (TAG) der Länge 128 Bit verwendet. Die asymmetrische RSA-Verschlüsselung des symmetrischen Schlüssels erfolgt mittels RSAES-OAEP, d.h. mittels Optimal Asymmetric Encryption Scheme gemäß RFC8017. Dabei kommt als Hash-Algorithmus SHA-256 (SHA-2) zum Einsatz, zur Maskenerzeugung wird MGF1 ebenfalls mit SHA-256 (SHA-2) verwendet. Entsprechend verschlüsselte Daten werden nach CMS/PKCS#7 erzeugt, d.h. konform zur Cryptographic Message Syntax gemäß RFC5083 und RFC5084 und schließlich im ASN.1-Format DER-kodiert an die Infrastruktur des Betreibers übertragen. Im Rahmen der Verschlüsselung werden alle Empfehlungen des aktuellen Stands der Technik gemäß RFC6160 umgesetzt.

Schlüsselerzeugung

Für die Erzeugung von symmetrischen Schlüsseln der Länge 256 Bit aus (eingegebenen oder über ein Identity-Management-System abgerufenen) Nutzerdaten kommt die Key Derivation Function PBKDF2 mit 100.000 Iterationen zum Einsatz. Ein Salt wird mangels Quelle dafür nicht verwendet.

Transportverschlüsselung

Jede Form der Datenübertragung wird generell über eine TLS-Transportverschlüsselung abgesichert, ältere SSL-Versionen sind in der Kommunikation nicht zugelassen. Das verwendete X.509-Zertifikat wird in kurzen Zeitabständen neu generiert. Für den Schlüsselaustausch bei Verbindungsaufbau wird Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) mit den Kurven X25519, P-256, P-384 und P-521 bevorzugt angeboten. Für alle Nutzer der Web-Anwendung kommt HTTP Strict Transport Security (HSTS) mit einer Mindestdauer von zwei Jahren zum Einsatz.

Kontakt

Falls Sie Fragen, Anregungen oder Probleme haben, zögern Sie nicht, mit uns in Kontakt zu treten. Wir werden uns gerne um Ihr Anliegen kümmern und stehen Ihnen mit Rat und Tat zur Seite.

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