QRONITON

Sichere Kontaktnachverfolgung mit QR-Codes

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

Der IT-Dienst wurde im Austausch mit Gesundheitsbehörden und dem Robert Koch Institut entwickelt und genügt höchsten Datenschutzanforderungen. Kontaktdaten der Nutzer sowie die mit Hilfe von Scans erfassten Kontaktketten werden mehrfach verschlüsselt und bleiben bis hin zu konkreten Infektionsfällen unzugänglich. Durch eine Zeit/Ort-abhängige Verschlüsselung wird sichergestellt, dass ausschließlich die Kontaktdaten direkt betroffener Nutzer mit akutem Infektionsrisiko eingesehen und an Gesundheitsbehörden weitergegeben werden können.

Bei der Nutzung des IT-Dienstes werden generell nur so wenige personenbezogene Daten erfasst, wie zur Bewältigung der Corona-Krise unbedingt erforderlich. Eine Verarbeitung und Weitergabe von personenbezogenen Daten erfolgt ausschließlich im Rahmen dieses expliziten gesellschaftlichen Zwecks und unter Einhaltung aller geltenden gesetzlichen Bestimmungen. Unter keinen Umständen werden personenbezogene Daten an unberechtigte Dritte, d.h. an Dritte außerhalb der Verantwortlichkeit des Betreibers oder des Gesundheitssystems, weitergegeben. Im Zuge einer externen Prüfung der Lösung wurde die Auftragsdatenverarbeitung mit QRONITON als unbedenklich eingestuft.

Die eingesetzten Verschlüsselungstechniken beruhen auf dem neuesten Stand der Technik und schließen Missbrauch und Manipulation von Daten aus. Das Konzept ist äußerst robust gegenüber illegitimen Zugriffsversuchen – insbesondere durch die beteiligten Parteien selbst. Ein Zugriff auf unverschlüsselte Daten durch den Betreiber des IT-Dienstes bleibt zu jedem Zeitpunkt ausgeschlossen. Anwendungsfehler sowie gezielte Angriffe von Außenstehenden werden durch zahlreiche Sicherheitsmechanismen verhindert. Das Verschlüsselungskonzept wurde von unabhängigen Kryptologen überprüft, durch Offenlegung des Quellcodes sind weitere Audits jederzeit möglich.

Mit diesem Dokument werden die datenschutzrelevanten Abläufe in QRONITON bei der Erhebung und Nachverfolgung von Kontaktketten für jeden Interessierten nachvollziehbar beschrieben.

Erhebung von Daten

Personenbezogene Daten

Im Zuge der Erstbenutzung wird die Telefonnummer des Nutzers und dessen Nutzerkennung über einen externen Campus-Login verknüpft. Aus den angegebenen Daten wird ein Nutzerschlüssel für die Verschlüsselung von Kontakt-Scans abgeleitet, der im Infektionsfall von der Hochschule rekonstruiert und als Einstiegspunkt für die Kontaktnachverfolgung herangezogen werden kann. Zum Zwecke einer Risikobewertung durch zuständige Gesundheitsbehörden wird vom Nutzer – stets auf freiwilliger Basis – auch dessen Postleitzahl abgefragt. Alle personenbezogenen Daten werden unmittelbar auf dem Gerät bzw. im Browser des Nutzers verschlüsselt und hernach an die Infrastruktur des Betreibers übertragen. Auf Nutzerwunsch lassen sich Registrierungsdaten darüber hinaus mit einem PIN-Code gegen Missbrauch

absichern. Zu statistisch-epidemiologischen Zwecken und zur Verbesserung des Dienstes wird die Postleitzahl (sofern angegeben) für den Betreiber zugänglich mit übertragen. Alle weiteren erhobenen Datenpunkte können nur durch den Schlüssel der Hochschule entschlüsselt werden und bleiben für den Betreiber dauerhaft unzugänglich. Jedem Nutzer steht zudem die Möglichkeit zur Offline-Teilnahme mittels Erzeugung eines ausdruckbaren personalisierten QR-Codes frei. Über die Web-Anwendung können auch digitale QR-Codes für spontane Zusammenkünfte mit einer Gültigkeit von 24 Stunden erzeugt werden. In beiden Varianten werden die verschlüsselt übertragenen Registrierungsdaten des Nutzers mit den Daten des jeweiligen QR-Codes ohne Rückbezugsmöglichkeit für den Betreiber, d.h. ebenfalls verschlüsselt, miteinander verknüpft.

Standortbezogene Daten

Für eine durch die Hochschule autorisierte Nutzergruppe steht weiterhin auch die Erzeugung von standortbezogenen QR-Codes offen. Im Zuge dessen werden standorttypische Daten, wie Postleitzahl, Gebäude und Beschreibung, abgefragt. Standortbezogene QR-Codes beinhalten in der darin eingebetteten Web-URL die angegebenen Standortdaten zur Anzeige bei Scan-Vorgängen. Entsprechende Daten werden bei der Erzeugung von QR-Codes analog zu personenbezogenen Daten unmittelbar auf dem Gerät des Nutzers verschlüsselt und ohne Personenbezug an die Infrastruktur des Betreibers übertragen. Zu statistisch-epidemiologischen Zwecken und zur Verbesserung des Dienstes wird die Postleitzahl des Standortes dem Betreiber zugänglich gemacht. Rückschlüsse auf Personen oder konkrete Gebäude bleiben für den Betreiber ausgeschlossen.

Kontakterfassung durch Scans

Durch Scannen eines QR-Codes werden die personenbezogenen Daten des jeweiligen Nutzers mit den personen- oder standortbezogenen Daten des gescannten QR-Codes verknüpft. Im Zuge dessen wird ein sekundengenauer Zeitstempel erzeugt und die voraussichtliche Dauer und Intensität des Kontakts über eine Auswahlliste abgefragt. Im resultierenden Datensatz werden für den Betreiber unzugängliche Verweise auf die verschlüsselten Kontaktdaten des scannenden Nutzers und die verschlüsselten Standortdaten des QR-Codes übertragen. Diese Verweise werden mit dem Hochschulschlüssel und zusätzlich mit einem 30 Minuten gültigen Zeit/Ort-abhängigen Schlüssel gesichert, der selbst wiederum mit dem Nutzerschlüssel verschlüsselt ebenfalls mit übertragen wird. Zu statistisch-epidemiologischen Zwecken werden anonyme Scan-Informationen, d.h. Kontaktdauer und Kontaktintensität sowie die Postleitzahl des Standortes, für den Betreiber zugänglich mit übertragen.

Verknüpfung von Kontakt-Scans

Mehrere Nutzer zur selben Zeit am selben Ort verwenden denselben Zeit/Ort-abhängigen Schlüssel zur Verschlüsselung von Scan-Daten und hinterlegen diesen mit ihrem Nutzerschlüssel gesichert in den resultierenden Datensätzen. Nach Rekonstruktion eines Nutzerschlüssels im Infektionsfall durch die Hochschule werden alle vom betroffenen Nutzer verwendeten Zeit/Ort-abhängigen Schlüssel und darüber die Scan-Daten unmittelbarer Kontaktpersonen mit gemeinsamen Aufenthalten zugänglich. Die darin enthaltenen Verweise auf verschlüsselte Nutzer- und Standortdaten lassen sich in einem weiteren Schritt mit Hilfe des Hochschulschlüssels rekonstruieren. Weitere Aufenthalte betroffener Nutzer, die nicht in Verbindung mit dem Infektionsfall stehen, bleiben dagegen unzugänglich, da diese mit anderen, nicht bekannten Zeit/Ort-abhängigen Schlüsseln erhoben wurden.

Speicherung von Daten

Vorhaltung auf Nutzergeräten

Auf dem Endgerät des Nutzers, d.h. in dessen persistentem Browser-Speicher, werden von der Web-Anwendung benötigte Schlüssel- und Steuerungsdaten ohne Personenbezug vorgehalten. Sofern angegeben wird auch die Postleitzahl des Nutzers mit abgelegt, um die erhobenen Datensätze neben dem Hochschulschlüssel auch mit dem Schlüssel der für den Wohnort des Nutzers zuständigen Gesundheitsbehörde verschlüsseln zu können. Darüber hinaus werden Informationen zum zuletzt gescannten QR-Code als Scan-Nachweis vorgehalten. Zu informativen Zwecken werden ferner auch die Gesamtzahl aller gescannten QR-Codes sowie Durchschnittswerte über 14 Tage für die Zahl an Kontaktpersonen und Kontaktstunden auf dem Gerät des Nutzers gespeichert und kontinuierlich aktualisiert. Eine Übertragung dieser Informationen an den Betreiber erfolgt nicht, ebenso ist daraus kein Rückschluss auf frühere besuchte Standorte möglich. Auf Nutzerwunsch lassen sich die gespeicherten Statistikdaten jederzeit zurücksetzen oder vollständig deaktivieren.

Übertragung an die Infrastruktur des Betreibers

Jeder an die Infrastruktur des Betreibers übertragene Datensatz wird neben der Verschlüsselung mit dem Hochschulschlüssel und etwaigen weiteren Zeit/Ort-abhängigen Schlüsseln grundsätzlich auch mit einem zusätzlichen Schlüssel des Betreibers gesichert, so dass ausschließlich nicht unterscheidbare Datensätze übertragen und somit der Einsatz eines Cloud-Anbieters zur Annahme der Daten ohne Risiko möglich ist. Die Teilentschlüsselung der Datensätze durch den Betreiber erfolgt dabei erst in dessen eigener Infrastruktur auf speziell gesicherten Systemen. Jede Form der Datenübertragung wird darüber hinaus auch mit einer zusätzlichen Transportverschlüsselung abgesichert. Die Vorhaltung von personenbezogenen Scan-Daten in der IT-Infrastruktur des Betreibers ist grundsätzlich auf 28 Tage begrenzt, ältere Kontakt-Scans werden kontinuierlich gelöscht.

Datenvorhaltung ohne eindeutige Identifikatoren

In den übertragenen Datensätzen finden sich keinerlei für den Betreiber zugängliche Identifikatoren oder anderweitig gleichbleibende Merkmale, aus denen sich ein Bewegungsprofil – auch nicht in pseudonymer Form – ableiten ließe. Dies wird durch eine konsequente Entkoppelung registrierter Nutzer- und Standortdaten von kontinuierlich erhobenen Scan-Daten über verschlüsselte Verweise sowie durch eine fortwährende Zeit/Ort-abhängige Neuverschlüsselung entsprechender Scan-Daten vor jeder Übertragung gewährleistet. Durch einen in die Verschlüsselungstechnik eingebetteten Zufallsanteil sind auch aufeinanderfolgende Scans einzelner Nutzer diesen nicht zuordenbar.

Einwilligung zur Datenerhebung

Bei Aufruf der Web-Anwendung werden ohne Zustimmung des Nutzers keinerlei personenbezogene Daten generiert oder erhoben. Es werden insbesondere keine Server-Logs vorgehalten oder IP-Adressen des Aufrufers protokolliert. Auf den Einsatz von Web-Analysediensten Dritter, auf Werbemittel oder andere Formen der besucherbasierten Monetarisierung wird dabei ebenso wie auf die Einbindung von externem Quellmaterial gänzlich verzichtet. Eine Erhebung von personenbezogenen Daten erfolgt nur mit ausdrücklicher Einwilligung des Nutzers im Rahmen der Registrierung. Mit jedem vom Nutzer durchgeführten Scan-Vorgang wird eine Zeit/Ort-beschränkte Einwilligung zur Nutzung der personenbezogenen Daten im Infektionsfall abgegeben, die gemäß Infektionsschutzgesetz mit einer Frist von vier Wochen durch Aufruf einer entsprechenden Funktion in der Web-Anwendung widerrufen werden kann. Der Betreiber verpflichtet sich zudem, alle erhobenen Scan-Daten kontinuierlich nach 4 Wochen zu

löschen. Lokal im Browser-Speicher vorgehaltene Daten können auf Wunsch des Nutzers jederzeit über die entsprechende Funktion in der Web-Anwendung oder durch Leeren des Browser-Storage gelöscht werden.

Verarbeitung von Daten

Betreiber

Die Erzeugung von anonymen QR-Code-URLs sowie von zeitabhängigen Schlüsselkomponenten erfolgt zentralisiert auf speziell dafür vorgesehenen Server-Systemen, während standortabhängige Schlüsselkomponenten zur Hinterlegung in den QR-Code-URLs lokal auf den Geräten der jeweiligen Nutzer generiert werden. Eine Speicherung bzw. Protokollierung von Informationen auf diesen Schlüssel-Servern, insbesondere von Identifikatoren, Schlüsselkomponenten, IP-Adressen oder auch konkreten Zeitpunkten der Schlüsselerzeugung, wird nicht vorgenommen. Alle verarbeiteten Daten werden ausschließlich flüchtig im Arbeitsspeicher der Server-Systeme vorgehalten und nicht mit den verschlüsselt erhobenen Nutzer- oder Standortdaten korreliert. Der Betreiber verpflichtet sich, diese Maßnahmen dauerhaft umzusetzen. Ungeachtet dessen würde eine unbefugte Erhebung entsprechender Server-Protokolle aufgrund der konsequenten Verwendung weiterer, für den Betreiber stets unzugänglicher, Schlüsselanteile zu keiner Schwächung des Datenschutzkonzepts führen. Vertrauen in die Integrität der Betreiberinfrastruktur ist daher generell nicht erforderlich. Die Entgegennahme von verschlüsselten personen- und standortbezogenen Daten sowie von Scan-basierten Kontaktverknüpfungen wird über davon unabhängige Server-Systeme des Betreibers realisiert, die über keine Kommunikationskanäle zu den Schlüssel-Servern verfügen. Da im vorliegenden Datenschutzkonzept ausschließlich eine Übertragung von mehrfach verschlüsselten Datensätzen vorgesehen ist, die sich zudem nur punktuell im Infektionsfall und unter Kooperation von Hochschule und Betreiber entschlüsseln lassen, ergeben sich für die Server-Infrastruktur des Betreibers keinerlei sicherheitsrelevante Bedenken. Die Verwendung eines in Deutschland ansässigen Cloud-Anbieters ist für diese Zwecke daher unkritisch. Die Erstentschlüsselung der entgegengenommen Datensätze durch den Betreiber, d.h. die Generierung und Aufbereitung von statistischen Informationen, erfolgt dagegen ausschließlich auf Betreiber-internen Systemen in dessen eigener Infrastruktur, die sich in einem zugangsgesicherten Rechenzentrum in Frankfurt befindet. Gleiches gilt für die Auslieferung der (nach wie vor mit dem Hochschulschlüssel verschlüsselten) Datensätze an den Hochschulverantwortlichen im Rahmen einer Kontaktnachverfolgung im Infektionsfall.

Hochschule

Verantwortliche der Hochschule können anhand der Telefonnummer oder Campus-Kennung einer infizierten Person deren Nutzerschlüssel rekonstruieren und darüber die Infektionsnachverfolgung auslösen. In der Folge werden vom Betreiber die mit dem Hochschulschlüssel verschlüsselten Registrierungsdaten an den Browser des Verantwortlichen zurückgeliefert und dort entschlüsselt. Die Korrektheit der für den Nutzerschlüssel hinterlegten Kontaktdaten ist durch den Verantwortlichen zu prüfen und zu bestätigen. Über die im Anschluss identifizierten Scan-Schlüssel des betroffenen Nutzers werden hernach alle Kontakt-Scans von Personen zur selben Zeit am selben Ort aufgefunden, zurückgeliefert und ebenfalls im Browser des Verantwortlichen entschlüsselt. In einem letzten Schritt erfolgt die Auslieferung und Entschlüsselung der Registrierungsdaten aller so identifizierten Kontaktpersonen. Um Missbrauch vorzubeugen, kann aus diesen Daten ein eindeutiger, für jeden Nutzer individueller Autorisierungs-Code abgeleitet werden, der den betroffenen Nutzern in der Web-Anwendung ebenfalls zur Verfügung steht. Über einen Abgleich des Autorisierungs-Codes kann der betroffene Nutzer somit die Kontaktaufnahme des Verantwortlichen legitimieren. Darüber hinaus stehen

dem Verantwortlichen selbst Prüfsummen über die registrierten Nutzer- und Standort-daten sowie über die von den Nutzern bei Registrierung und Scan-Vorgängen eingegebenen PIN-Codes (falls vergeben) zur Verfügung, worüber ein Missbrauch der Kontakterfassung seitens Dritter zuverlässig erkannt werden kann. Der Betreiber erlangt dabei zu keinem Zeitpunkt Einsicht in entschlüsselte Datensätze, gleich welcher Art, protokolliert aber den Zeitpunkt jeder Nachverfolgungsanfrage, um Missbrauch seitens der Hochschule vorzubeugen.

Gesundheitsbehörden

Die aus der Nachverfolgung resultierenden Kontaktdaten direkt betroffener Nutzer sind naturgemäß zur Weitergabe an die zuständigen Gesundheitsbehörden bestimmt. Anhand der Postleitzahl der jeweiligen Nutzer (sofern angegeben) lassen sich die Kontaktdaten zielgerichtet verteilen, andernfalls erfolgt eine Weitergabe an die am Standort der Hochschule zuständige Behörde. Auf Wunsch der Hochschule kann darüber hinaus auch ein Direktzugriff für Gesundheitsbehörden eingerichtet werden. In diesem Fall werden alle erhobenen Daten, d.h. Registrierungsinformationen für Nutzer und Standorte sowie Kontakt-Scans, neben dem Schlüssel der Hochschule auch mit dem Schlüssel der zuständigen Behörde gesichert. Dieser Schlüssel wird anhand der Postleitzahl ermittelt, so dass angeschlossene Behörden ausschließlich Datensätze in ihrem Zuständigkeitsbereich entschlüsseln können. Alle Sicherheitsgarantien, insbesondere hinsichtlich des rein fallbezogenen Datenzugriffs zum Schutz unbeteiligter Nutzer und Nutzeraufenthalte bleiben weiterhin gültig.

Epidemiologen

Zu statistischen Zwecken, insbesondere zur Beobachtung der Effektivität von Eindämmungsmaßnahmen, sowie zum Zwecke weiterführender Forschungsarbeiten über die Ausbreitung des Corona-Virus werden vollständig anonymisierte, d.h. standortbezogen aggregierte Datensätze ohne jedweden Personenbezug erzeugt. Diese Datensätze werden vom Betreiber zur Verbesserung des Dienstes herangezogen sowie an berechtigte Stellen, z.B. vom Robert Koch Institut ausgewiesene Epidemiologen oder Forschungseinrichtungen, weitergegeben. Entsprechend weitergegebene Daten beinhalten ausschließlich aggregierte Informationen nach Postleitzahl. Mit Hilfe dieser Forschungsdaten ist eine anonyme Auswertung von Kontakt-Clustern, regionalen Häufungen, Ausbreitungsmustern etc. ohne Rückschluss auf einzelne Nutzer und damit eine Verbesserung der Pandemiebekämpfung möglich.

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. Die nachfolgende Beschreibung der einzelnen Schritte der Verschlüsselung 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 30-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 Nutzerangaben 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

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 128 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 rekonstruierbarer Quelle 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.