Änderung der TLS-Zertifikatskette 03.12.2024/04.12.2024

Bei Problemen: Support kontaktieren

Für den Fall, dass Sie am 03.12.2024/04.12.2024 in Folge der TLS-Zertifikatsumstellung auf unerwartete Fehler stoßen, kontaktieren Sie bitte umgehend unseren Support über support@divera247.com oder telefonisch über 0202 37322660

Am Dienstag, den 03.12.2024 wird das verwendete TLS-Zertifikat für die Domain divera247.com ausgetauscht. Insbesondere betroffen hiervon sind:

- www.divera247.com (Marketing-Website)
- app.divera247.com (Web-App + API)
- ws.divera247.com (Echtzeitaktualisierung)

Das neue Zertifikat wird durch D-Trust GmbH, ein Unternehmen der deutschen Bundesdruckerei bereitgestellt.

Getestete Unterstützung für Geräte

iOS

Betriebssystem	Unterstützung	Echtzeitaktualisierung
iOS 11 (2017) und älter	nicht getestet	nicht getestet
iOS 12 (2018)	✅	✅
ab iOS 13+ (2019)	✅	✅

✅ = Unterstützung wurde durch uns getestet

Alarmgeber

Alarmgeber Download & Installation

Android

Betriebssystem	Unterstützung	Echtzeitaktualisierung
Android 4 und älter	nicht getestet, von der App nicht mehr unterstützt	nicht getestet
Android 5 und 6 (2015)	⚠️ Workaround notwendig	❌ alle 60 Sekunden
Android 7 (2016)	✅	✅
ab Android 8 (2017)	✅	✅

⚠️ = Workaround notwendig

✅ = Unterstützung wurde durch uns getestet

Android-App Workaround bei Fehler SSL-Handshake

Betrifft: Android 6 (und älter)

Ab Android App Version 2.2.51 können Sie versuchen, gültige SSL Zertifikate auf dem Gerät zu installieren, in dem Sie im Loginschirm ganz unten auf "Probleme mit SSL? hier klicken" klicken.

Veraltete Betriebssysteme

Warnung: Das verwendete Betriebssystem ist stark veraltet

Hilfe im Fehlerfall

Die Webseite divera247.com kann seit der Umstellung nicht mehr aufgerufen werden

Für den unwahrscheinlichen Fall, dass Sie unsere Webseite unter www.divera247.com nicht mehr aufrufen können, und Ihnen eine Fehlermeldung angezeigt wird, dass keine sichere Verbindung aufgebaut werden kann, haben Sie folgende Möglichkeiten.

Betriebssystem und Browser aktualisieren

Prüfen Sie auf Aktualisierungen Ihres Betriebssystems (Windows/macOS/Linux/Android/iOS), sowie Ihres verwendeten Browsers (Firefox/Google Chrome/Edge).

Das Betriebssystem, sowie der Browser bringen die vertrauenswürdigen Zertifikate mit. Eine Aktualisierung erneuert ebenfalls die vertrauen Zertifikate.

D-Trust GmbH Root-Zertifikate manuell vertrauen

Die Root-CA Zertifikate der D-Trust GmbH finden Sie im Repository-Bereich (https://www.d-trust.net/de/support/repository) unter "Veröffentlichte Zertifikate" > "Ausstellende CAs" > "TLS-Zertifikate".
Relevant sind dabei die folgenden beiden:

Direktlink: D-TRUST SSL CA 2 2020 D-Trust (Root-CA:Root Class 3 CA 2 2009)
SHA-1 Fingerprint: AEB9682B91D20B50384A2C6B6DACBB851F629962

Direktlink: D-TRUST Root Class 3 CA 2 2009 (PEM- und DER-Zip)

Nach dem Download können Sie diese per Doppelklick auf das Zertifikat zu Ihren vertrauten Zertifikaten hinzufügen. Alternativ verwenden Sie die in Ihrem Browser integrierte Funktion zum Zertifikatsimport.

Vollständige Zertifikatskette manuell vertrauen

Sie können ebenfalls unsere aktuelle vollständige Zertifikatskette herunterladen und dieser vertrauen.

SHA-256 Checksum: 57d48b0e51190f55e09f28b6eb140a00a3a434784b716b0eca5a00440832cc75

Alarmgeber (Windows Programm) zeigt javax.net.ssl.SSLHandshakeException:

Wichtiger Hinweis: Der Alarmgeber wurde 2018 durch zentrale Auswertungsmechanismen ersetzt, was die Zuverlässigkeit durch das Hosting im Rechenzentrum (ISO-zertifiziert, Standort in Deutschland) erhöht und den Einrichtungsaufwand für Sie auf ein absolutes Minimum reduziert.

Zur Auswertung von E-Mails empfehlen wir den Alarmserver. Zur Auswertung der DME-Datenausgabe BosMon.

Das Windows-Programm "Alarmgeber" wird seit 2018 nicht mehr unterstützt. Die dahinterstehende Softwaretechnologie ist Anfang 2019 durch den Hersteller komplett vom Markt genommen worden, sodass es uns auch nicht mehr möglich ist, Updates für den Alarmgeber zu erstellen. Uns ist es zwar in der Vergangenheit mehrfach gelungen, Workarounds für den Alarmgeber zu erstellen, wir haben das auch bei dieser Änderung für die Handvoll verbleibenden Alarmgebernutzer versucht, das scheint in diesem Fall aber aussichtslos.
Spätestens mit der für uns verpflichtenden Unterstützung von TLS 1.3 im Februar wäre der Alarmgeber nicht mehr nutzbar geworden.
Die Sicherheit der in DIVERA 24/7 verarbeiteten Daten lässt hier wenig Spielraum für die Nutzung uralter Sicherheitsarchitektur und -Technologie