

Nutzung der Push-Dienste von Apple / Google

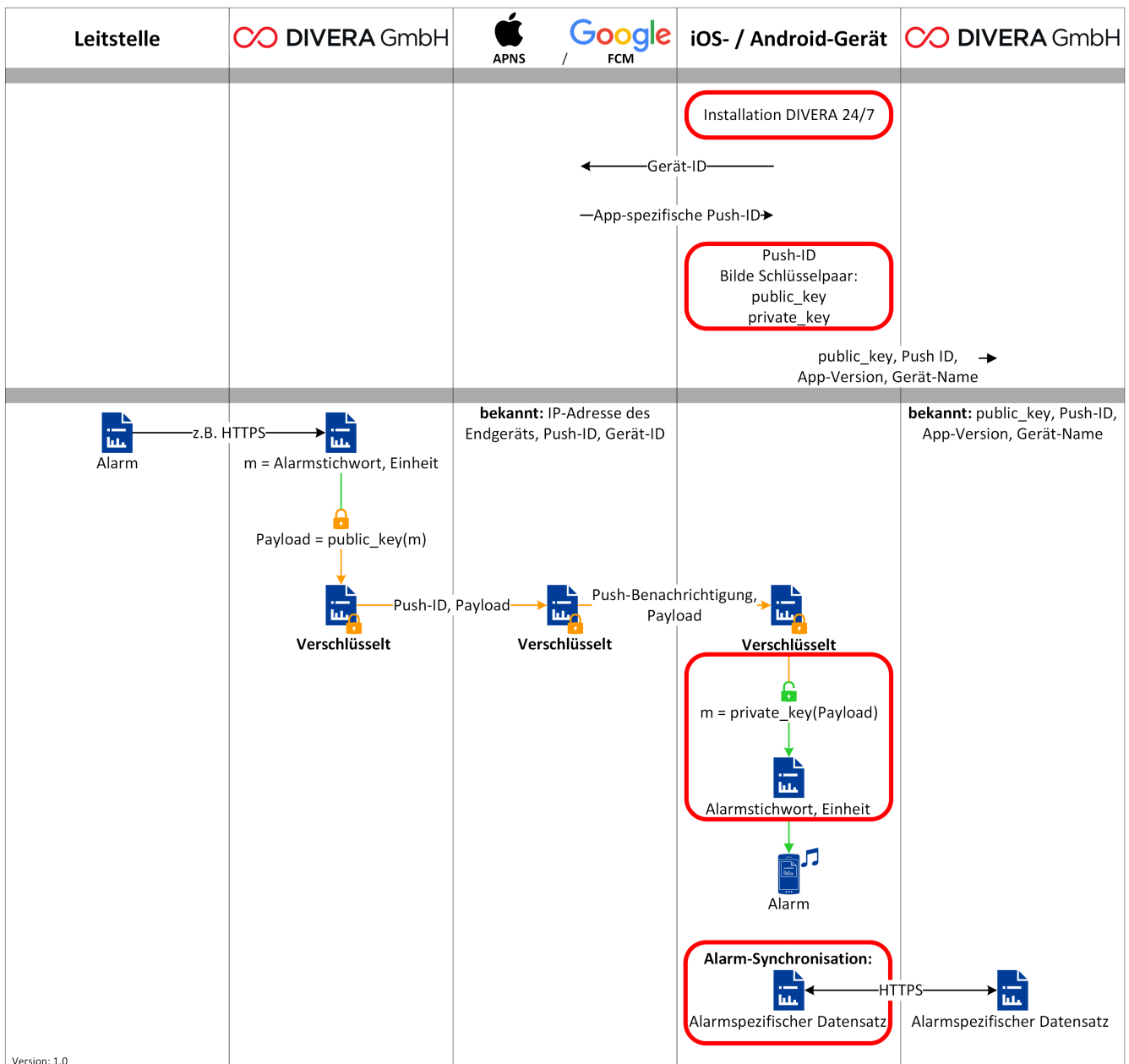
Die DIVERA 24/7-App nutzt die Push-Dienste der Betriebssystemhersteller. Das sind Kurzmitteilungen, die mit Einwilligung der Nutzer:in auf dessen Display angezeigt werden. Mit diesen Push-Mitteilungen wird die App-Nutzer:in über Einsätze, Benachrichtigungen, etc. informiert. Im Fall der Nutzung der Push-Dienste wird ein Device-Token von Apple oder eine Registration-ID von Google zugeteilt (Push-ID). Zweck deren Verwendung durch uns ist allein die Erbringung der Push-Dienste. Es handelt sich hierbei nur um anonymisierte, App-spezifische IDs. Rechtsgrundlage der Datenverarbeitung ist Art. 6 Abs. 1 lit. b DS-GVO.

Während der Installation der App können Sie entscheiden, ob Sie diese Funktion nutzen wollen. Eine spätere Abmeldung der Push-Nachrichten ist über die Einstellungen Ihres mobilen Endgerätes möglich.

Ablauf

Die folgende Abbildung zeigt, wie eine Alarmierung über die Push-Dienste von Apple / Google an ein mobiles Gerät gesendet wird.

Der obere Teil zeigt die Installation der DIVERA 24/7-App. Von Apple / Google wird eine App-spezifische Push-ID vergeben, mit dieser DIVERA 24/7 die jeweiligen Apps / Geräte ansprechen kann. Außerdem bildet die DIVERA 24/7-App ein asymmetrisches Schlüsselpaar zur Ende-zu-Ende-Verschlüsselung. Den öffentlichen Schlüssel, die Push-ID, die App-Version und den Gerätenamen überträgt das Gerät per HTTPS an DIVERA 24/7. Die App-Version und der Gerätenamen wird im jeweiligen Benutzerkonto hinterlegt, um der Benutzer:in die verknüpften Geräte anzeigen zu können. Auch können die verknüpften Geräte im Benutzerkonto entfernt werden.



Der untere Teil visualisiert den Ablauf einer Alarmierung. DIVERA 24/7 erhält den Alarm von der Leitstelle und verschlüsselt das Alarmstichwort und die Einheit mit dem öffentlichen Schlüssel der Benutzer:in. Dieser Payload wird zusammen mit der hinterlegten Push-ID an Apple (APNS) / Google (FCM) gesendet. *Durch die Ende-zu-Ende-Verschlüsselung hat Apple / Google keine Kenntnis über das Alarmstichwort und die Einheit. Apple / Google kennen aber folgende Informationen: die IP-Adresse des Geräts, die Push-ID und die Gerät-ID.* Der Payload wird anschließend von der DIVERA 24/7-App mit dem privaten Schlüssel entschlüsselt und in der Push-Benachrichtigung angezeigt. Außerdem wird ggf. ein Alarmsignal abgespielt. Im Anschluss synchronisiert sich die App wie gewohnt per HTTPS direkt mit DIVERA 24/7, ohne Umwege über Apple / Google.

Datenschutz-Bewertung

Apple (APNs)

Apple erstellt, verarbeitet und speichert die Gerät-ID sowie die Push-ID und kann diese auch dem jeweiligen Nutzer zuordnen. Außerdem verläuft die Kommunikation über die Server von Apple, sodass Apple auch noch die üblichen Verbindungsdaten (IP-Adresse) kennt. Zusätzlich wird der Inhalt der Push-Nachricht (Payload), über Apple hinweg Ende-zu-Ende verschlüsselt, übertragen. Die Push-ID, in der Funktion ähnlich einer E-Mailadresse, können wir natürlich nicht vor Apple geheim halten.

Da Apple empfiehlt, nicht aber erzwingt (!), dass der Inhalt der Nachricht verschlüsselt wird, sehen Sie sich nicht als Auftragsverarbeiter. Aus unserer Sicht sind aber bereits die Push-ID und die Verbindungsdaten personenbezogene Daten. Diese Daten fallen immer bei der Verwendung eines Apple Endgerätes an, unabhängig ob der Endnutzer jetzt DIVERA 24/7 verwendet oder nicht.

Bei der Datenverarbeitung übermittelt die Apple Distribution International Ltd. (Hollyhill Industrial Estate, Hollyhill, Cork, Republic of Ireland) Daten an die Apple Inc. (One Apple Park Way, Cupertino, CA 95014, USA). Apple stützt die Übermittlung auf Modul 2 der EU-Standarddatenschutzklauseln (Datenübermittlung Verantwortlicher an Auftragsverarbeiter). Apple sieht sich also als verantwortliche Stelle und nicht als Auftragsverarbeiter.

Informationen in der iOS App

Push-Dienste sind Server die Nachrichten (ähnlich SMS) an Apps übertragen. Diese App nutzt sie z.B. für die Alarmierung.

Dafür verwenden wir den für iOS-Geräte notwendigen Apple Push Notification Service (APNs), einen Dienst der Apple Inc. in den USA. Bei der Verwendung von APNs wird auf dem Gerät eine Installations-ID erstellt und übertragen, um zu bestimmen an welche Geräte Push-Nachrichten zugestellt werden müssen. Dies ist für die Nutzung des Push-Dienstes erforderlich.

Die Inhalte der Push-Benachrichtigungen sind sicher Ende-zu-Ende verschlüsselt.

Datenschutz und Sicherheit bei APNs: <https://www.apple.com/legal/privacy/de-ww/>

Details zu den geltenden Datenschutzbestimmungen von Apple: <https://www.apple.com/de/privacy/>

Google Firebase Cloud Messaging (FCM)

Oben genannter Sachverhalt trifft auch auf die Verwendung von Google Firebase Cloud Messaging (FCM) zu, allerdings mit dem Unterschied, dass Google sich im Gegensatz zu Apple als Auftragsverarbeiter sieht und einen entsprechenden AV-Vertrag bereitstellt.

Informationen in der Android App

Pushdienste sind Nachrichten, ähnlich SMS, die Server an Apps übertragen. Die DIVERA 24/7 Android App nutzt sie z. B. für die Alarmierung.

Dafür verwenden wir den für Androidgeräte üblichen Pushdienst Firebase Cloud Messaging (FCM), einen Dienst der Google Group in den USA. Bei der Verwendung von FCM wird auf dem Gerät eine Installationsid erstellt und übertragen um zu bestimmen an welche Geräte Nachrichten zugestellt werden müssen. Dies ist für die Nutzung des Pushdienstes unabdingbar.

Die Inhalte der Push-Benachrichtigungen sind sicher Ende-zu-Ende verschlüsselt.

Details zu den geltenden Datenschutzbestimmungen von Google: <https://firebase.google.com/support/privacy>