Sicherheit und Datenschutz – aPager PRO

Übersicht

Dieses Dokument beschreibt die Verschlüsselung von **aPager PRO** und Android und iOS. Das Dokument ist gültig ab FE2 Version **2.16** und wurde zuletzt aktualisiert am 18.05.2021.

Standort

Alle verwendeten Server werden in Frankfurt, Deutschland betrieben.

Verschlüsselung

Die verschlüsselte Übertragung und das verschlüsselte Abspeichern kritischer Daten ist ein essentielles Sicherheitskriterium. Hierbei nutzen wir verschiedene Techniken um das größte Maß an Sicherheit zu gewährleisten.

Transportverschlüsselung

Alle Informationen zu unserem Server werden über HTTPS transportverschlüsselt.

„HTTPS wird zur Herstellung von Vertraulichkeit und Integrität in der Kommunikation zwischen Webserver und Webbrowser (Client) im World Wide Web verwendet. Dies wird unter anderem durch Verschlüsselung und Authentifizierung erreicht.

Ohne Verschlüsselung sind Daten, die über das Internet übertragen werden, für jeden, der Zugang zum entsprechenden Netz hat, als Klartext lesbar. Mit der zunehmenden Verbreitung von offenen (d. h. unverschlüsselten) WLANs nimmt die Bedeutung von HTTPS zu, weil damit die Inhalte unabhängig vom Netz verschlüsselt werden können.

Die Authentifizierung dient dazu, dass beide Seiten der Verbindung beim Aufbau der Kommunikation die Identität des Verbindungspartners überprüfen können. Dadurch sollen Man-in-the-Middle-Angriffe und teilweise auch Phishing verhindert werden.“[1]

Ende-zu-Ende Verschlüsselung

Vor allem die Ende-zu-Ende Verschlüsselung über ein asymmetrisches Verfahren garantiert die vollständig sichere Übertragung von Ihrem lokalen System auf das Endgerät des Nutzers. Nur durch eine Ende-zu-Ende Verschlüsselung kann gewährleistet werden, dass zu keiner Zeit ein unbefugter Zugang zu Ihren sensiblen Daten hat. Auch für uns als Betreiber ist kein Zugriff auf die verschlüsselten Daten möglich.

[1] https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

Die Verschlüsselung ist keine Option, sondern passiert im Hintergrund vollautomatisch. Den genauen Ablauf können Sie dem unten stehenden Diagramm entnehmen.

Dateiverschlüsselung

Der von uns verwendete Cloud Anbieter verwendet mehrere Stufen der symmetrischen Verschlüsselung um den physikalischen Zugriff auf Festplatten zu erschweren.

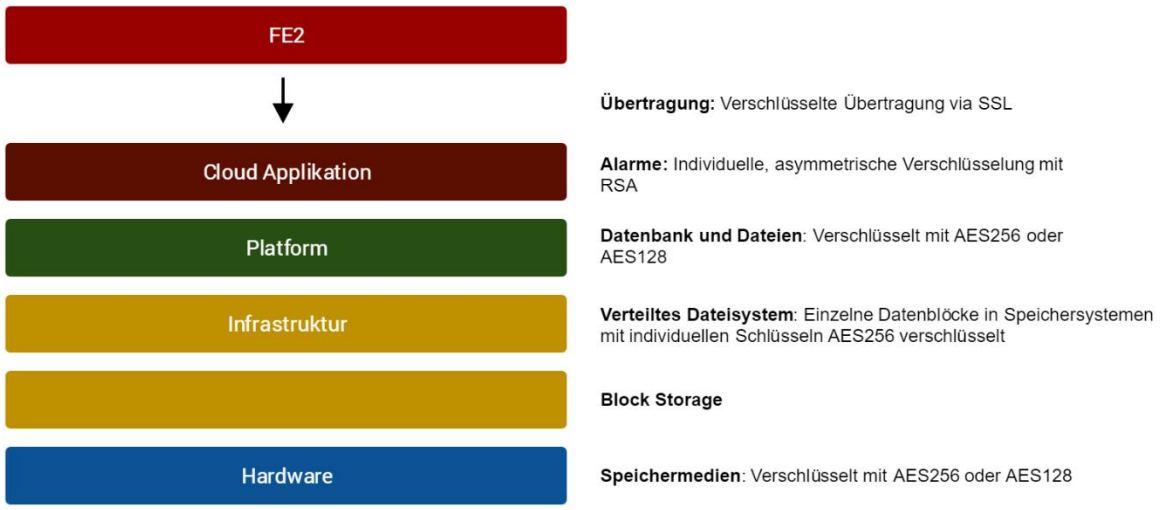

Abbildung 1 Verschlüsselungsstufen, Quelle Google LLC

Ablauf

In Abbildung 2 wird der Ablauf der Verschlüsselung näher erläutert. Zu Beginn einer Alarmierung landet ein Alarm, egal von welcher Quelle, unverschlüsselt in FE2. Solange dieser nur im lokalen Netzwerk verbleibt, ist eine Verschlüsselung nicht zwingend notwendig. Spätestens jedoch, wenn ein Alarm über Drittnetze (z.B. Internet) nach außen gelangt, so muss eine Verschlüsselung angewandt werden.

Hierzu wird der Alarm zuerst symmetrisch mit einem zufälligen Passwort verschlüsselt (AES/CBC/PKCS5Padding; Schlüssellänge AES 256 Bit). Anschließend wird das Passwort individuell für jeden aPager PRO Empfänger mit dessen öffentlichen Schlüssel asymmetrisch verschlüsselt (RSA/ECB/PKCS1Padding; Schlüssellänge RSA 2048 Bit). Der verschlüsselte Text in Kombination mit den jeweiligen verschlüsselten Passwörtern werden anschließend transportverschlüsselt (HTTPS) an unseren Server übertragen.

Alle Empfänger werden anschließend über Push informiert, dass neue Alarme vorhanden sind. Die Push-Nachrichten werden hierbei von den jeweiligen Herstellern (Apple, Google) verschickt. Der Push selbst enthält, je nach Empfänger, folgende Informationen:

- Android
    - Eindeutige Datenbank-ID zum späteren Abruf. Keinerlei Nutzdaten
- iOS

- Keinerlei Nutzdaten

Bei Erhalt der Push-Nachricht, ruft die App wieder über eine gesicherte HTTPS Verbindung die offenen Alarme ab. Dieser Zugriff wird über einen individuellen Zugriffschlüssel des Geräts geschützt. Beim erfolgreichen Abruf werden diese sofort vom Server gelöscht und können dort auch nicht wiederhergestellt werden. Auf dem Endgerät kann das Passwort nun mit dem privaten Schlüssel des Nutzers asymmetrisch entschlüsselt und anschließend die Nutzdaten mit dem Passwort symmetrisch entschlüsselt werden.

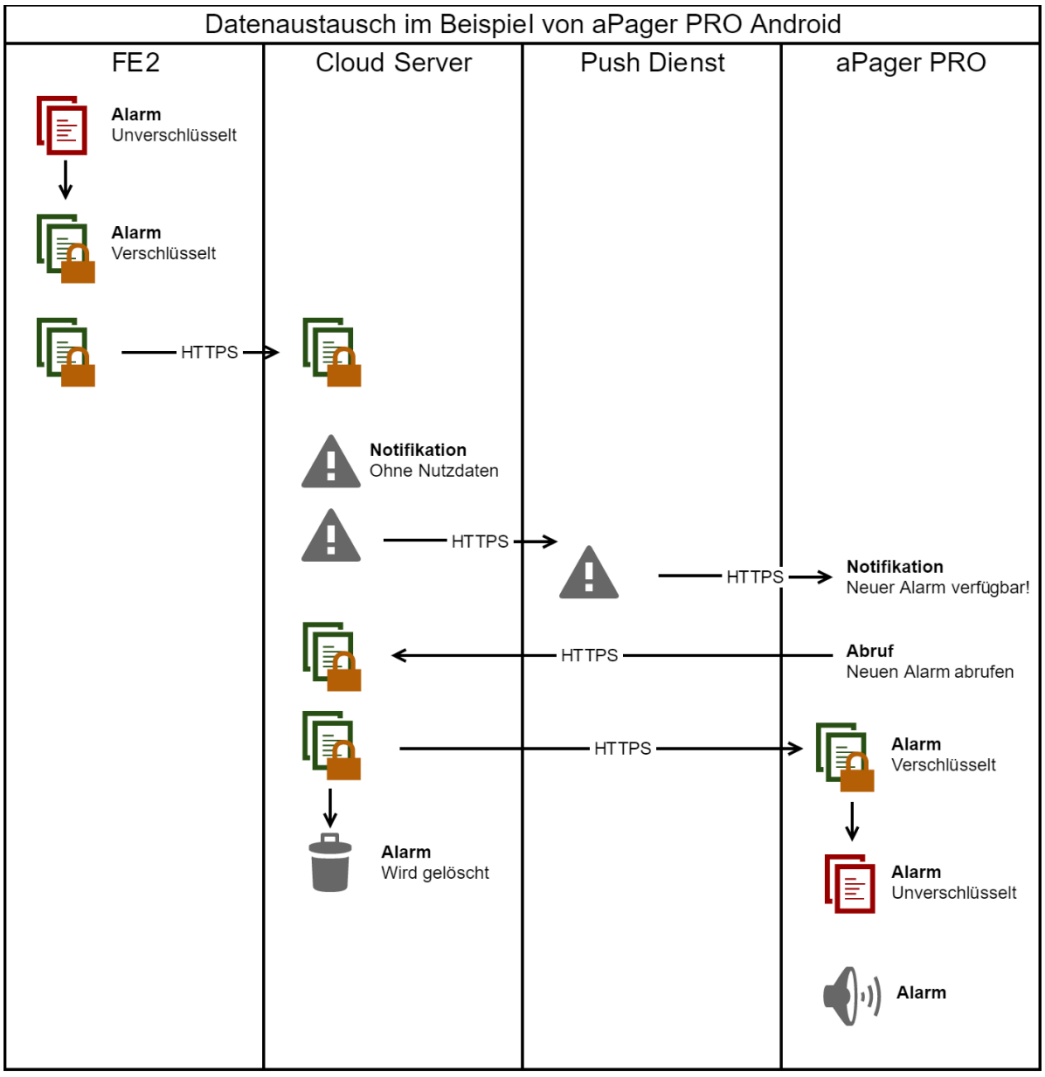

Abbildung 2 Verschlüsselungsablauf

Empfängerkreis

Wer welchen Alarm empfangen kann wird in FE2 festgelegt. Dort wird die vom Nutzer verknüpfte E-Mail-Adresse hinterlegt. Der Nutzer muss über den Klick auf einen Link in einer Aktivierungs-E-Mail bestätigen, dass er Zugriff auf die von ihm verknüpfte E-Mail-Adresse hat. Ansonsten werden keine Nachrichten zugestellt. Die E-Mail-Adresse dient nur zur Identifikation des Nutzers, Nachrichten werden nicht per E-Mail verschickt.

Der Nutzer kann **nicht** selbst entscheiden, welche Nachrichten er erhalten möchte.

Auf Grund der asymmetrischen Verschlüsselung, können die Empfänger nur die für sie bestimmten Nachrichten entschlüsseln. Ohne den entsprechenden privaten Schlüssel, kann kein Zugriff auf das Passwort und somit die Nutzdaten erfolgen.

Datenspeicherung

Nachfolgend informieren wir Sie über Art und Umfang der gespeicherten Daten.

Alarme

Die Alarme müssen auf einem zentralen Server zwischengespeichert werden, damit diese von aPager PRO abgerufen werden können.

Der Alarm wird so lange gespeichert, bis er abgerufen wird. Nach Abruf des Alarms von aPager PRO wird der Alarm sofort vom Server gelöscht und kann auch später nicht mehr abgerufen werden.

Da Alarme symmetrisch verschlüsselt sind, landen keine Nutzdaten auf dem Server. Ein Alarm besteht ausfolgenden relevanten Informationen:

Feld	Bedeutung
`Encryption`	Dieses Feld steht immer auf true (Existenz wegen Historie)
`Gruppe`	Der Einheitenname der alarmierten FE2 Einheit
`Inhalt`	Der bei iOS anzuzeigende Text in der Notifikation im Klartext
`iv`	Verwendeter Initialisierungsvektor für AES
`salt`	Verwendetes Salt; für jeden Alarm neu generiert
`Verschlüsselte Nachricht`	Eigentliche Nutzdaten symmetrisch verschlüsselt
`Signatur`	Signatur von FE2 über verschickte Nutzdaten
Pro Empfänger	
`aPagerPRO`	Empfänger Email Adresse
`Telefonnummer`	Empfänger Handy Nummer für Rückfallebene (optional)

`Verschlüsseltes Passwort`	Asymmetrisch verschlüsseltes Passwort
`Public RSA Key`	Verwendeter Public Key

Nachrichten, die älter als **7 Tage** sind, werden automatisch vom Server gelöscht, selbst wenn aPager PRO die Alarme noch nicht abgerufen hat.

Registrierungen

Für jeden aPager PRO Nutzer müssen folgende Informationen gespeichert werden:

Feld	Bedeutung	Optional
`Authentifizierung`	Automatisch generierter Schlüssel zur Authentifizierung gegenüber der Schnittstelle des zentralen Servers	Nein
`Gerätetyp`	ANDROID für Android Geräte und IOS für iOS Geräte	Nein
`Email`	Die verknüpfte Email Adresse des Nutzers	Nein
`Push Token`	Der Push Token der jeweiligen Hersteller	Nein
`Authentifiziert`	Ob dieser Nutzer seine Email authentifiziert hat oder nicht. Sollte er diese nicht authentifiziert haben, kann der Nutzer keine Alarm empfangen	Nein
`Push Status`	Ob der Versand der Push Nachrichten deaktiviert worden ist oder nicht	Nein
`Lizenz`	CLIENT für clientseitige Lizenzierung und SERVER für serverseitige Lizenzierung	Nein
`Profile`	Vom Nutzer angelegte Profile mit Name der Einheit und Auswahl des Klingeltons	Ja
`Änderungsdatum`	Änderungsdatum	Nein
`Registrierungsdatum`	Registrierungsdatum	Nein
`Funktionen`	Liste von Funktionen (Online Services)	Ja
`Gruppen`	Liste von zugehörigen Gruppen (Online Services)	Ja

Name	Name der Person (Online Services)	Ja
Geheimnis	Zugriffstoken zur Veränderung der Verfügbarkeit oder Rückmeldungen (Online Services)	Nein
Letzte Aktualisierung	Änderungsdatum der Verfügbarkeit (Online Services)	Nein
Verfügbarkeit	Status der Verfügbarkeit (Online Services)	Nein

Zertifizierungen

Der von uns verwendete Cloud Anbieter wurde nachfolgenden Standards zertifiziert:

- ISO 27001
  - Dies ist einer der bekanntesten international anerkannten unabhängigen Sicherheitsstandards. Sämtliche Systeme, Anwendungen, Mitarbeiter, Technologien, Prozesse und Rechenzentren, die zur Bereitstellung der Cloud Plattform eingesetzt werden, sind nach ISO 27001 zertifiziert.
- ISO 27017
  - Cloud Security: Dies ist ein speziell auf Clouddienste ausgerichteter internationaler Anwendungsstandard für Maßnahmen zur Informationssicherheit auf der Basis von ISO/IEC 27002.
- ISO 27018
  - Cloud Privacy: Dies ist ein internationaler Anwendungsstandard für den Schutz personenbezogener Daten in öffentlichen Clouddiensten
- DS-GVO (GDPR)
  - Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden.

Weitergabe an Push-Dienste

Für die Push Alarmierung werden die nativen Push Dienste von Google (GCM bzw. FCM) und Apple (FCM bzw. APNS) verwendet.

Diese sind für die Signalisierung der Alarme notwendig und werden folgendermaßen genutzt:

Android (Google)

Hier wird via Googles Push Dienst lediglich ein „Alarm ist da“ Signal verschickt. Es werden keine Nutzdaten (der eigentliche Alarm selbst) übermittelt.

iOS (Apple)

Hier wird via Googles Push Dienst lediglich ein „Alarm ist da“ Signal verschickt. Es werden keine Nutzdaten (der eigentliche Alarm selbst) übermittelt.

Auch hier sind alle Dienste via Transportverschlüsselung (HTTPS) angebunden.