

# e:LION Einsatzdokumentation



## SSL Webserver und Datenübergabe

Status 3 IT GmbH

01/2020

## 1.1 Einrichtung SSL Webserver

Ab Version 5.5 enthält der e:LION Server einen voll funktionsfähigen SSL (HTTPS) Webserver. Dieser kann auch dazu genutzt werden, um Einsätze, Fahrzeug-Status und Fahrzeug-Positionen von externen Diensten an e:LION zu übergeben. Derzeit wird diese Funktion von Divera247 sowie FeuerSoftware Connect unterstützt.

Um den Server zu aktivieren müssen ein paar Parameter in der Datei „Server.cfg“ angelegt werden.

Zuerst muss der SSL-Server im e:LION-Server mit dem Konfigurationseintrag

```
SSLServerPort=443
```

aktiviert werden. Anstatt 443 kann auch jeder freie TCP Port verwendet werden. Wichtig ist, dass dieser TCP-Port des Servers über das Internet erreichbar ist. Hierzu muss i.d.R. eine Port-Weiterleitung auf dem Internet-Router des Standortes eingerichtet werden.

Das im e:LION Server enthaltene Zertifikat ist „selbst-signiert“ und erzeugt beim Aufruf über einen Webbrowser eine Sicherheitswarnung. Um das zu umgehen kann auch ein eigenes Zertifikat verwendet werden. Diese wird mit den Einstellungen

```
SSLServerCertFile=NameDerDatei.pfx
```

```
SSLServerCertPW=Passwort
```

Konfiguriert.

In jedem Fall muss noch mindestens ein Benutzer des Typs „4“ konfiguriert werden. Z.B.

```
User=test|xyz123|4|ABCDEFGHOpqrst9876xxx|7.001F.010.00|7.001F|_7
```

Konfiguriert den http Benutzer „test“ mit Passwort „xyz123“ und Web-Schlüssel „ABCDEFGHOpqrst9876xxx“, primäre Gruppe „7.001F.010.00“, Schreibrechte auf Gruppen beginnend mit „7.001F“ und Leserechten auf alle Gruppen beginnend mit „7“.

Als Web-Schlüssel sollte eine ausreichend lange und zufällige Zeichenfolge (mind. 50 Zeichen) gewählt werden.

Nach Änderungen an der Server.cfg muss der e:LION Server neu gestartet werden.

Zur Prüfung, dass der SSL Server ordnungsgemäß funktioniert, kann die die URL des Servers im Web-Browser aufgerufen werden. Dieser sollte dann nach Eingabe von Benutzernamen und Passwort die Datei ‚index.html‘ aus dem Unterordner „html“ anzeigen.



## 1.2 Konfiguration DIVERA247

Um Einsätze von Divera247 zu e:LION zu Übertragen muss unter [divera47.com](http://divera47.com) der „Request Service“ aktiviert werden. Über die Menüs Verwaltung->Einstellungen->Schnittstellen->Datenübergabe kann der Request-Service aktiviert werden (nicht verfügbar in der FREE-Version von DIVERA). Dort muss die URL des e:LION Servers eingetragen werden (öffentlich erreichbare Adresse des eigenen e:LION Servers sowie der verwendete Port. Der Dateiname des Requests ist `/API/DIVERA/einsatz.json?userkey=<meinWebSchlüssel>`

Der Userkey/Webschlüssel muss mit dem aus der `Server.cfg` übereinstimmen.

Als Format ist „POST application/json“ einzustellen und als Inhalt „Vollständiges Objekt (incl. Empfänger)“.

The screenshot shows the configuration page for the 'REQUEST-SERVICE' in the DIVERA247 interface. The page has a dark blue header with 'Abbrechen' and 'Speichern' buttons. Below the header is a navigation bar with tabs: 'ALARMIERUNG', 'MITTEILUNGEN', 'ALARMSERVER', 'REQUEST-SERVICE' (selected), and 'WEITERE SCHNITTSTELLEN'. The main content area contains the following elements:

- A heading: "Der erzeugte Alarm-Datensatz kann über einen GET- oder POST-Aufruf automatisch an einen externen Dienst übergeben werden."
- A checked checkbox: "Alarmierung automatisch weiterleiten"
- A text input field labeled "URL/Ziel des Requests" containing the URL: `https://mein-elion-server.de:44399/API/DIVERA/einsatz.json?userkey=ABHijklmnnxxxxopq123ewradsaf`
- A dropdown menu labeled "Format" with the selected value: "POST application/json"
- A dropdown menu labeled "Inhalt" with the selected value: "Vollständiges Objekt (inkl. Empfänger)"
- A "Wichtiger Hinweis" (Important Note) at the bottom: "Der Request wird parallel zur Verarbeitung und Benachrichtigung über die App-internen Mechanismen durchgeführt. Der Request wird nicht protokolliert und im Fall eines Fehler **nicht automatisch** wiederholt. Verwenden Sie zur sicheren Übertragung nach Möglichkeit **https**."

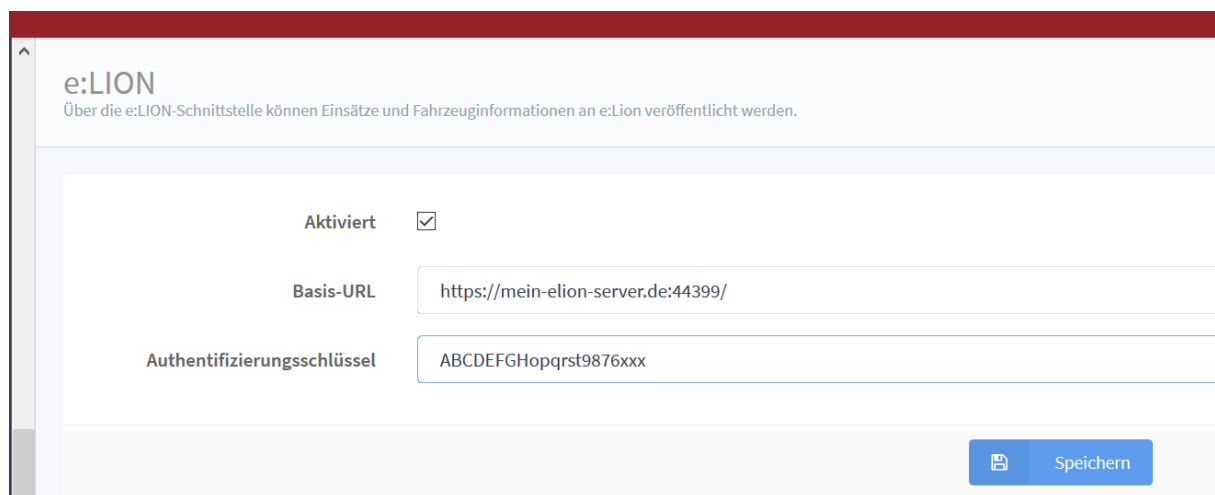
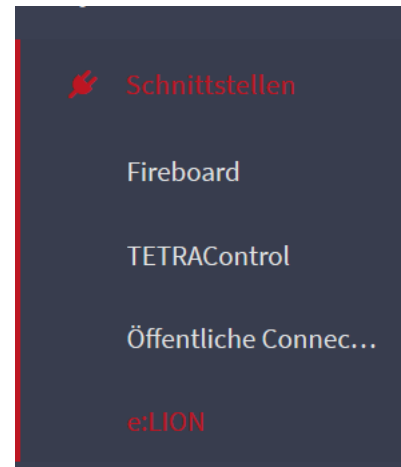
### 1.3 Konfiguration FeuerSoftware CONNECT

Aus FeuerSoftware Connect können Einsätze sowie Status und Positionen die von der App gesendet werden an e:LION übertragen werden.

Im Connect muss die e:LION Schnittstelle aktiviert werden.

Die Basis-URL ist die öffentliche Adresse des e:LION Servers incl. Port (muss aus dem Internet erreichbar sein).

Unter „Authentifizierungsschlüssel“ muss der Web-Schlüssel des SSL Benutzers aus der Server.cfg eingetragen werden.



Damit die Status und Positionen den Fahrzeugen korrekt zugeordnet werden können, muss die Kennung des jeweiligen Tablets entweder mit der FMS-Kennung des Fahrzeugs aus der Datei „FMS.csv“ übereinstimmen, oder die Kennung muss einer der ISSIs aus den TETRA Geräten des Fahrzeugs (ebenfalls aus der FMS.csv) entsprechen.

Die Datei FMS.csv muss sich im Verzeichnis des e:LION Servers befinden, damit diese eingelesen werden kann.

