LPWAN BENUTZERHANDBUCH

Status: Veröffentlicht

Version 1.03 vom **27.09.2023**

Wien Energie GmbH
FN 215854H
UID-Nr.: ATU55685501

iot@wienenergie.at

Inhaltsverzeichnis

Vorwort

Dieses Handbuch dient Wien Energie Kunden mit dem Produkt „**LPWAN Konnektivität**“ einen Überblick über die Konfigurationsmöglichkeiten der unterschiedlichen Applikationen des LPWAN Servers. Neben einer Beschreibung der Funktionalitäten und Möglichkeiten werden mit Hilfe von bebilderten Beispielen exemplarisch die notwendigen Schritte von der Erstellung eines Endkundengeräts am Netzwerkserver, bis zur finalen Datenübertragung über den LPWAN Applikationsserver an ein externes Kundensystem (z.B. IoT Plattform), beschrieben. Zudem wird auf die zur Verfügung gestellte API-Schnittstelle näher eingegangen.

Sollten Sie eine individuelle Beratung wünschen, oder haben Sie spezifische Fragen zu möglichen Umsetzungen, kontaktieren Sie uns unter der E-Mail-Adresse iot@wienenergie.at.

Änderungshistorie

Version	Änderungen	Erstellungs-/Änderungsdatum	Status
1.03	Finalisierung	2023.09.27	Veröffentlicht

1. Darstellung der LPWAN Architektur

Abbildung 1 zeigt die Leistungsgrenzen (orange Markierung) für das zugrunde liegende LPWAN Konnektivitätsprodukt. Angeboten wird der Empfang der LPWAN Datenpakete der registrierten Endkundengeräte, die Weiterleitung ebendieser Datenpakete bis einschließlich unseres Applikationsservers am LPWAN Netzwerkserver sowie die Bereitstellung der Daten über standardisierte Datenschnittstellen wie zB. MQTT; HTTPS Protokoll oder ähnlich. Die Datenübertragung erfolgt über Wien Energie LPWAN Outdoor Gateways an exponierten Funkstandorten im Versorgungsgebiet, welche eine gesicherte Verbindung zum redundanten LPWAN Server besitzen. Im Bedarfsfall können für kundenspezifische Use-Cases Indoor Gateways an Kundenstandorten installiert werden. LPWAN Indoor Gateways werden ausschließlich auf Basis gesonderter Bestellung zur Verfügung gestellt.

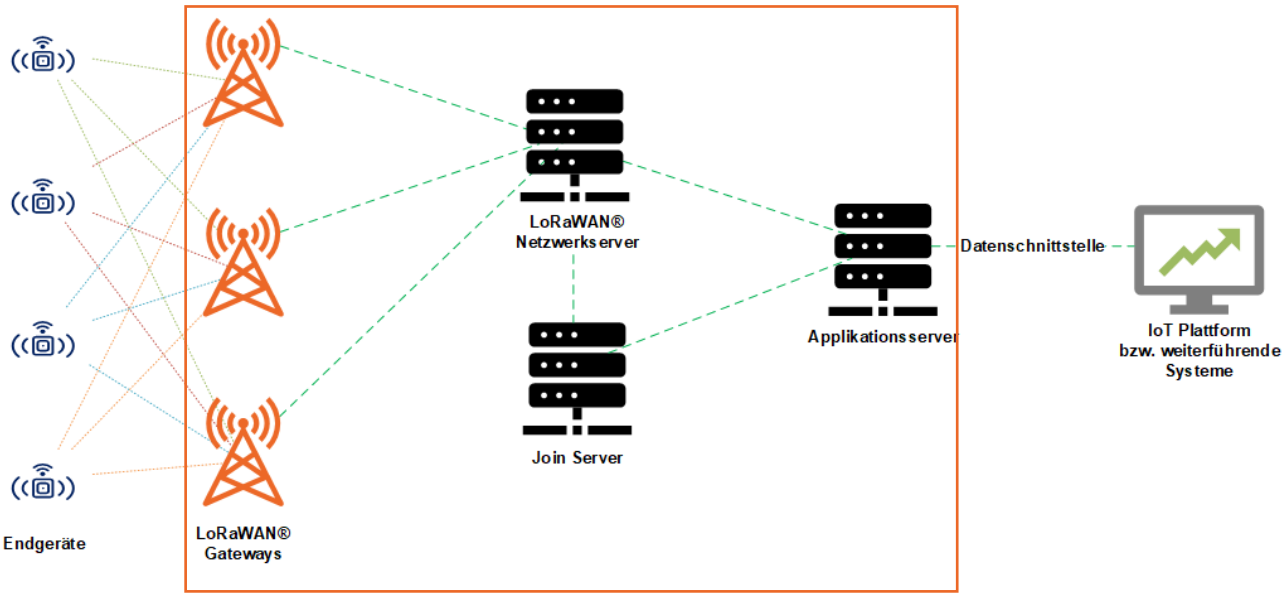

Abbildung 1: Leistungsgrenzen Wien Energie inkl. Datenschnittstellen

1.1 Zentrale Links (URL) - Zugänge und Dokumentation zum LPWAN Server

Der LPWAN Server stellt seine Services (Netzwerkserver, Applikationsserver) über unterschiedlichste Links (siehe URLs), geo-redundant im Versorgungsgebiet der Wien Energie zur Verfügung, wobei jeder Endkunde einen gesicherten Zugang in seinen eigenen Kundenbereich am System erhält. Der hierfür notwendige **Kundenlogin** (Benutzername), wird im Zuge der Fertigstellungsmeldung des Service durch Wien Energie an den Kunden schriftlich übermittelt.

Netzwerkserver	**Zentrales Kundenportal** zwecks Einrichtung/Verwaltung von Endkundengeräten/Benutzern	https://ui.lpwan.wienenergie.at/portal **siehe Kapitel 2**
	➢ **Device Manager** (Endkundengeräte verwalten)	https://ui.lpwan.wienenergie.at/deviceManager **siehe Kapitel 2.2**
	➢ **Wireless Logger** LoRaWAN® Datenpakete von Endkundengeräten	https://ui.lpwan.wienenergie.at/ThingPark/wlogger/gui **siehe Kapitel 2.4**
	Netzwerkserver Schnittstelle (API) Programmierschnittstelle (API) zum LPWAN Netzwerkserver zwecks Errichtung/Verwaltung/Abfrage von Endgeräten/Benutzern/Status	https://dx-api.lpwan.wienenergie.at/admin/latest/swagger-ui/index.html?shortUrl=tpdx-admin-api-contract.json **siehe Kapitel 2.5**
	Dokumentation der API-Befehle	https://dx-api.lpwan.wienenergie.at/thingpark/dx/core/latest/doc/
Applikationsserver	**Datenmanagementportal (ThingPark X)** zwecks Einrichtung/Verwaltung der Datenübertragungsendpunkte von Endkundengeräten, Nutzdatendekodierung sowie Datenstruktur	https://ui.lpwan.wienenergie.at/tpx/login **siehe Kapitel 2.3**
Allgemein	**LPWAN Empfangsstärke Check „Heatmap“** Wien Energie LPWAN IoT Heatmap zwecks Prüfung der Empfangsstärke im Versorgungsgebiet*****	https://heatamap.iot.wien

Tabelle 1: LPWAN Hyperlinks (URL)

***** LPWAN Signalstärketests können bei Bedarf von Endkunden mit geeigneten Endgeräten im Versorgungsgebiet der Wien Energie durchgeführt werden. Unter der Webadresse https://heatmap.iot.wien werden diese graphisch visualisiert und stehen öffentlich zur Verfügung. Bei Interesse hierzu kontaktieren Sie uns unter iot@wienenergie.at.

2. Aufbau des zentralen LPWAN Kundenportals

Unter dem LPWAN Kundenportal wird das zentrale Web-Interface verstanden, über das Kunden Zugriff auf die Ihnen zugewiesenen Geräte und Lizenzen erhalten. Neben der Möglichkeit Endkundengeräte und Benutzer zu verwalten, können hiermit Datenpakete von/an Endkundengeräte eingesehen bzw. Daten an Endkundengeräte gesendet werden. Zudem ist es möglich, Aussagen zu LoRaWAN® Datenpaketen für die eigene Endkundengeräte einzusehen (Wireless Logger). Für jeden Endkunden wird zumindest ein Kundenadministrator in einem eigenständigen (autonomen) Kundenbereich erstellt. Die hierfür notwendigen Informationen werden von Wien Energie mittels „**Fertigstellungsmeldung**“ an die angeführte Kundenemailadresse der Bestellung versandt. Der Login durch den Kunden am Portal erfolgt mittels „**Benutzername**“ (E-Mailadresse) und selbst gewähltem „**Passwort**“. Der Link für die Aktivierung des Kundenkontos sowie die erstmalige Erstellung des Passworts wird via E-Mail zugesendet.

Abbildung 2 zeigt beispielhaft den Login am LPWAN Kundenportal nach Aktivierung des Kundenkontos und gesetztem Passwort für den Benutzer:
demouser@wienenergie.at

Abbildung 2: Loginmaske am Kundenportal

Nach dem Login ist der Administratorbenutzer in der Lage, selbstständig LoRaWAN® Endgeräte im **Device Manager** hinzuzufügen sowie mit dem **Wireless Logger** LoRaWAN® Datenpakete in der Luftschnittstelle einzusehen. Ebenso können weitere Benutzer („**End Users**“) mittels Zahnradsymbol – siehe **Abbildung 3** - am System hinzugefügt werden.

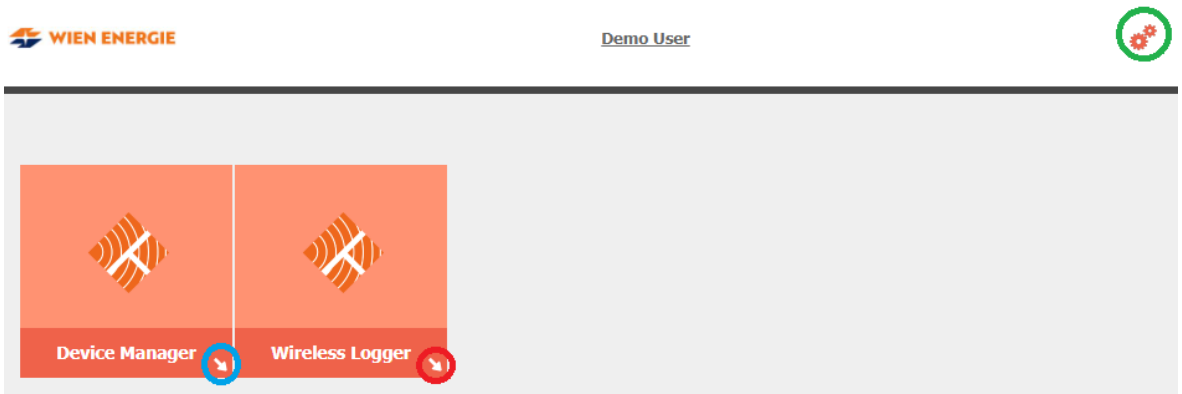

Abbildung 3: Kundenportal Applikationsübersicht

Um die unterschiedlichen Applikationen zu starten, klickt man die Pfeile (**blau** bzw. **rot**) der jeweiligen Applikation an. Für die Einstellungen oder das Anlegen von zusätzlichen Benutzern – **siehe Kapitel 2.1** - klickt man auf das Zahnradsymbol (**grün**).

2.1 Administration von Endkunden-Benutzern und Berechtigungen

Nach Klick auf das Zahnradsymbols und dem darauf erscheinenden Pop-up „**End Users**“, öffnet sich ein weiteres Fenster zur Erstellung bzw. Verwaltung von weiteren Endkundenbenutzern durch den jeweiligen Kundenadministrator. Der Kundenadministrator hat die notwendigen Rechte, neue Endkundenbenutzer auf unterschiedlichsten Ebenen (Administrator-/Benutzerlevel) sowie mit unterschiedlichster Berechtigung (Schreib-/Leserechte) zu erstellen.

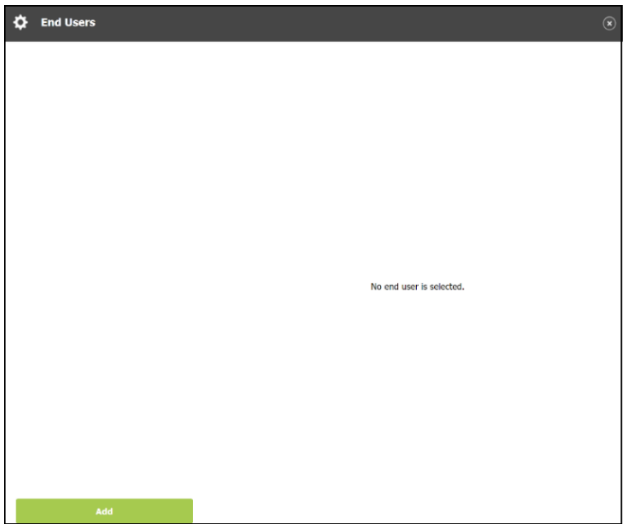

Abbildung 4: Übersicht konfigurierte Benutzer des Endkunden

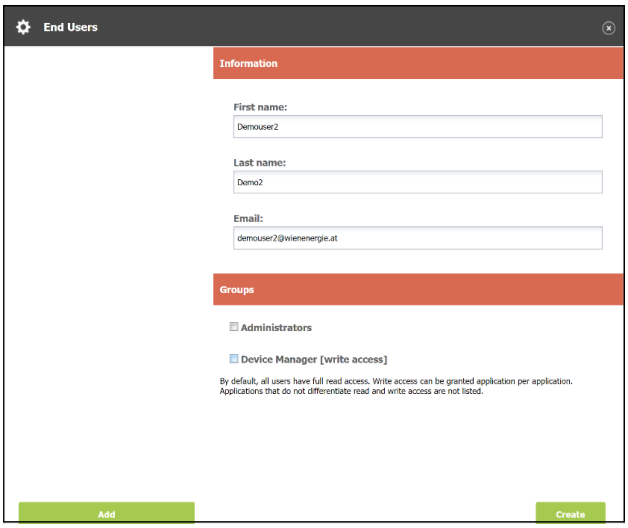

Abbildung 5: Erstellung Benutzer für Endkunden

In **Abbildung 4** sind sämtliche konfigurierte Endkundenbenutzer ersichtlich. Aktuell ist kein weiterer Benutzer angelegt. Um einen zusätzlichen Benutzer anzulegen, klickt man auf „**Add**“ und fügt den Benutzer mitsamt notwendigen Informationen – siehe **Abbildung 5** - hinzu. Im angeführten Beispiel wurde ein Benutzer ohne Administrator- und ohne Schreiberechte für den Device Manager (kein hinzufügen/editieren von Endkundengeräten) hinzugefügt.

Der neue Benutzer erhält ein E-Mail von lpwan@wienenergie.at mit einem Aktivierungslink, wo der neu angelegte Benutzer nach Klick auf die URL sein Passwort setzen kann.

BEACHTE:

- Der Aktivierungslink für neue Benutzer ist nach Erhalt des E-Mails (Erstellung des Benutzers) sieben Tage lang gültig und verfällt danach.
- Eine Passwortänderung (bereits aktivierter Benutzer) ist **48 Stunden** nach Erhalt der E-Mail gültig.
- Passwörter dürfen weder Vor- und Nachnamen enthalten und müssen mindestens **12** | maximal **32 Zeichen** lang sein.

Nach erfolgreicher Definition des Passworts, kann der neu angelegte Benutzer sich am zentralen Kundenportal mit seiner E-Mailadresse und seinem gewählten Passwort anmelden. Da im obigen Beispiel der Benutzer ohne Administratorrechte angelegt wurde, kann der Benutzer keine weiteren Endkundenbenutzer, als auch keine Endkundengeräte, anlegen. Der Zugriff auf die Applikation des Wireless Loggers ist im aktuellen Fall möglich, da für diese Applikation lediglich Leserechte notwendig sind.

Tipp: Sollten mehrere Benutzer mit derselben E-Mail angelegt werden, so kann dies mit einem „**+**“ Zeichen nach der E-Mail-Adresse erfolgen, um Benachrichtigungen auf nur eine E-Mail zu erhalten.

Beispiel: Ein bereits angelegter Benutzer hat die E-Mail demouser@wienenergie.at, so könnte ein weiterer Benutzer mit demouser+mustermann@wienenergie.at angelegt werden, wobei die E-Mail vor dem „**+**“ Zeichen (demouser@wienenergie.at) für den Versand von Aktivierungslinks bzw. zum Zurücksetzen des Passworts verwendet wird.

2.2 LPWAN Device Manager

Der LPWAN Device Manager ist die Applikation zur Errichtung/Verwaltung von LPWAN fähigen Endkundengeräten im Wien Energie LPWAN Netz. Hierzu werden durch den Kunden LPWAN Endgeräte mitsamt den notwendigen LPWAN Informationen erstellt/importiert und mit einer dazugehörigen Datenapplikation sowie einem Routingprofil verknüpft. Zudem bietet der Device Manager eine einfache und schnelle Übersicht für allgemeine Informationen zu allen Endgeräten eines Kunden (Datenpakete, Packet Error Rate, Batteriestatus etc.) an. Um etwaige Probleme in der Kommunikationsübertragung zu vermeiden, darf das jeweilige LPWAN Endkundengerät nur auf einer LPWAN Netzwerkserverinfrastruktur (zB. Wien Energie LPWAN Server) zur gleichen Zeit angelernt werden. Sollten dem Endkundengerät unterschiedlichen Netzwerkserver bekannt sein, so kann dies zu Fehlern in der Datenübertragung führen.

Weiters ist der Device Manager nicht dazu gedacht, herstellerspezifische Softwareeinstellungen auf den Endkundengeräten (Sensoren, Aktoren etc.) direkt vorzunehmen. Hierfür gibt es in der Regel eigene Software, die Sie bei den Herstellern erhalten. Manche LPWAN Endkundengeräte können (lediglich) mit Hilfe von LPWAN Downlink-Nachrichten konfiguriert werden, müssen jedoch üblicherweise zuvor am Wien Energie LPWAN Netzwerkserver erfolgreich eingebunden sein, um die Einstellungen an das Endkundengerät zu senden.

2.2.1 LPWAN Endkundengeräte erstellen

Nachdem das Pfeilsymbol beim LPWAN Device Manager geklickt wurde, öffnet sich ein neues Fenster, um Endkundengeräte anzulegen.

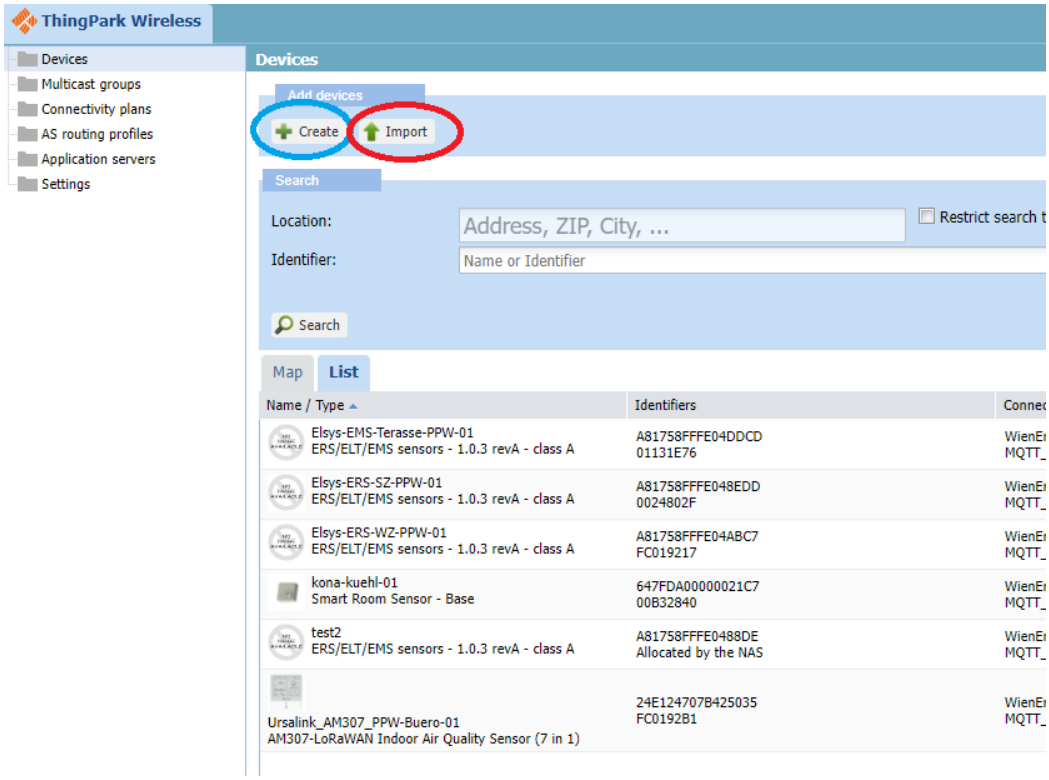

Abbildung 6: Übersicht Endkundengeräte

Endgeräte können entweder manuell (durch den Benutzer in der Oberfläche) mittels **Create** (**blau**) oder mit Hilfe einer **standardisierter Excel-Vorlage** (**rot**) angelegt/importiert werden. Ebenso kann die Verwendung der Programmierschnittstelle (API) – **siehe Kapitel 2.5** – zur Verwaltung von Endkundengeräten verwendet werden.

Sollten Sie Interesse an der standardisierten Excel-Vorlage haben, senden Sie uns bitte ein Mail an iot@wienenergie.at und wir übermitteln das Dokument an Sie.

2.2.2 Einzelne Endkundengeräte manuell erstellen

Durch Klick auf den „**Create“** (**blau**) Knopf öffnet sich ein neues Eingabefeld, wo die notwendigen Parameter zum jeweiligen Endkundengerät eingestellt werden können. Endkundengeräte benötigen zwecks weiterer Verarbeitung an Drittsysteme ein definiertes Routingprofil, das sowohl die gewünschte Endstelle als auch die Formatierung der Nutzdaten definiert. Um ein dementsprechendes **Routingprofil** zu erstellen, müssen die Parameter – **siehe Kapitel 2.2.5** – definiert werden.

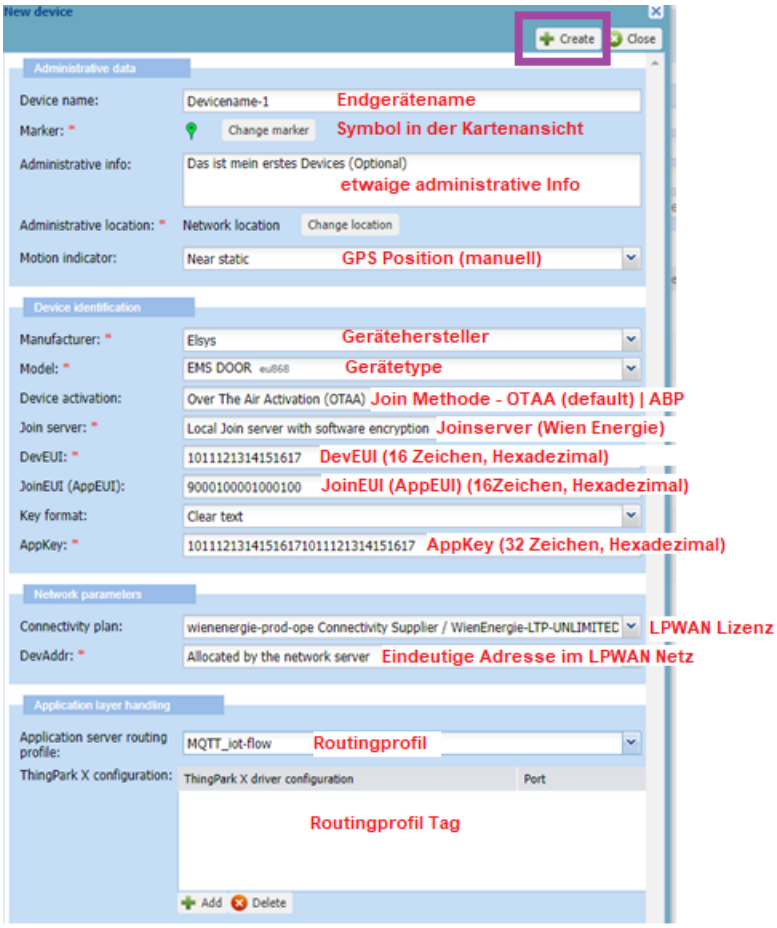

Abbildung 7: LPWAN Endgerät anlegen

Ein Klick auf „**Create**“ (**lila**) erstellt das Endgerät am LPWAN Netzwerkserver. Im Anschluss ist das angelegte LPWAN Endgerät in der Übersicht des Device Managers ersichtlich.

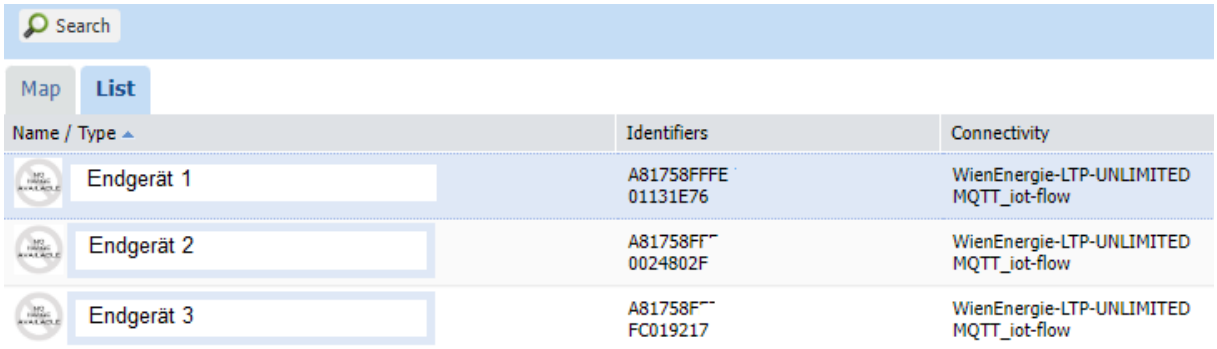

Abbildung 8: Endgeräte Übersicht in Listenform

2.2.3 (Einzelne) Downlinks an Endkundengeräte via GUI senden

Aus dem Device Manager heraus können schnell und einfach für einzelne Endgeräte Downlink-Nachrichten definiert und an Endkundengeräte gesendet werden. Hierfür sucht man im Device Manager das gewünschte Endgerät in der Statusübersicht aus und öffnet dies, indem man das Lupensymbol anklickt.

Abbildung 8: Endgeräteübersicht

Danach erscheint ein Fenster mit Statusinformationen zum ausgewählten Endkundengerät. Mit einem Klick auf „**Send downlink**“ öffnet sich ein Pop-up Fenster, wo die Downlink-Nachricht weiter spezifiziert werden kann.

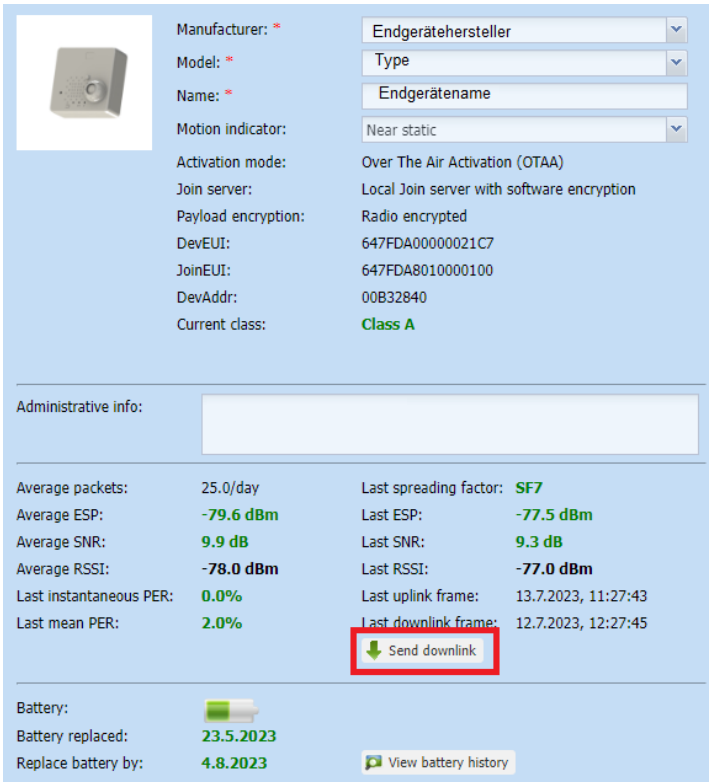

Abbildung 9: Send Downlink Knopf

Sämtliche Optionen für Downlink-Nachrichten entnehmen Sie bitte der Anleitung ihrer Endgerätehersteller. Mancher Hersteller stellt „**Downlink-Generatoren**“ auf seiner Webseite zur Verfügung. Exemplarisch: Hersteller Elsys.se für Elsys LPWAN Endgeräte.

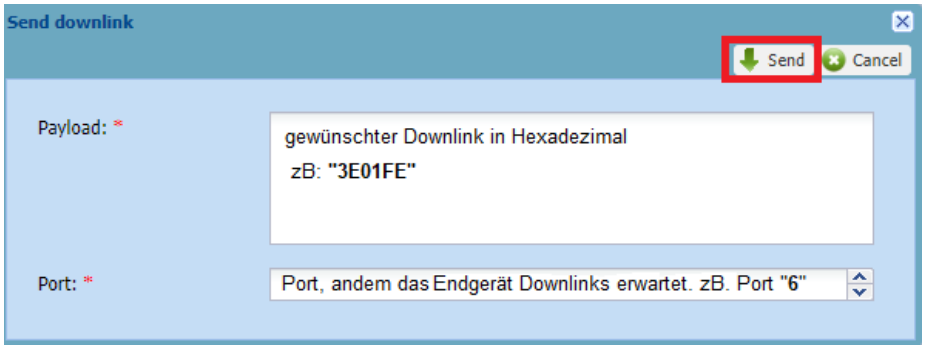

Abbildung 10: Downlink-Nachricht definieren

Nachdem der gewünschte Downlink definiert und mittels „**Send**“ übermittelt wurde, wird dieser in der „**Downlink-Warteschlange**“ („Queue“) am Netzwerkserver eingereiht. Bei **Class A** LPWAN Endgeräten öffnet sich, nachdem ein Endgerät einen Uplink (Nachricht vom Sensor zum Server) gesandt hat, ein Zeitfenster, wo der Sensor auf Downlink-Nachrichten durch den Server wartet. Da eine Downlink-Nachricht am Netzwerkserver für das Endgerät in der Warteschlange vorhanden ist, wird diese Nachricht an das Endgerät gesandt und kann vom Endgerät dementsprechend nach Erhalt verarbeitet werden.

Der erfolgreiche Versand kann zudem im „**Wireless Logger**“ – **siehe Kapitel 2.4** – eingesehen und verifiziert werden.

BEACHTE:

- Für das Senden von Downlink-Nachrichten aus dem Device Manager muss der jeweilige Endkundenbenutzer zumindest über Schreibrechte verfügen. Leserechte reichen dafür nicht aus!
- Für jedes einzelne Endkundengerät (eindeutige DevEUI) steht am Netzwerkserver eine Warteschlange für maximal **fünf (5) Downlinks** pro Endkundengerät zur Verfügung. Sollten fünf Downlinks für ein (1) Endgerät in der Warteschlange vorhanden sein und auf die Verarbeitung warten, so würde eine **sechste (6) Downlink-Nachricht** den jeweils ersten Downlink in der Warteschlange des Endgerätes überschreiben.

Tipp: Wien Energie empfiehlt Downlinks über die Netzwerkserver Schnittstelle (API) bzw. über eine konfigurierte ThingPark X Connection (zB. MQTT) zu senden, da neben der Möglichkeit für weitere Optionen auch eine Rückmeldung vom Netzwerkserver/Endgerät zum Erhalt der Downlink-Nachricht (**confirmed Messages**) zurückgegeben werden kann.

2.2.4 LPWAN Endgerätekompatiblität

Um Endkundengeräte erfolgreich im Wien Energie LPWAN Netzwerk zu betreiben, müssen beim Anlegen unterschiedlicher Endgeräte die hierfür notwendigen Kommunikationsparametereinstellungen der Endgerätehersteller (siehe Endgeräte-Beschreibungen) beachtet und am LPWAN Server eingestellt werden. Hierfür bietet der Wien Energie LPWAN Server (**Stand: 11.07.2023**) bereits für mehr als 462 unterschiedliche Endgerätetypen ein LPWAN Verbindungsprofil an. Grundsätzlich wird empfohlen, stets mit durch die LoRa Alliance® zertifizierten Endgeräten (LINK) zu arbeiten, um höchstmögliche Kompatibilität und Zuverlässigkeit zu gewährleisten. Sollten Endgerätehersteller bzw. Endgerätetypen nicht namentlich am Wien Energie LPWAN Server auswählbar sein, so können diese Endgeräte als „**Generic Device**“ mit der jeweiligen LoRaWAN ® Spezifikation angelegt und betrieben werden.

Wien Energie pflegt und erweitert die Endgeräteprofile in regelmäßigen Abständen und stellt diese Änderungen allen Kunden zur Verfügung. Trotz aller Sorgfalt kann es vorkommen, dass Endgerätetypen mit unterschiedlichem Firmwarestand von den Herstellern/Händlern ausgeliefert werden. Es empfiehlt sich daher, trotz gewähltem Endgerätetype/Profil einen ausgiebigen Test auf Funktionalität durchzuführen, bzw. im Wireless Logger die Datenpakete auf Funktionalität zu prüfen.

Wien Energie bietet zudem die kostenpflichtige Möglichkeit an, spezifische Endkundengeräte in Absprache mit dem Kunden zu testen und geeignete Endgeräteprofile zu erstellen. Hierfür nehmen Sie bitte mit iot@wienenergie.at Kontakt auf.

2.2.5 Erstellung von Routingprofilen zwecks Weiterleitung von Nutzdaten

Um die Nutzdaten (Payload) von Endgeräten an weiterführende externe Systeme von Dritten zu senden, bedarf es der Definition von zumindest einem „**AS-Routingprofil**“. Diese Einstellungen können für einzelne oder einer Vielzahl von Endgeräten verwendet werden.

Zu Beginn wird im Device Manager ein Routingprofil unter dem linken Menüpunkt „**AS Routing Profile**“ – **siehe Kapitel 2.2.5** - erstellt.

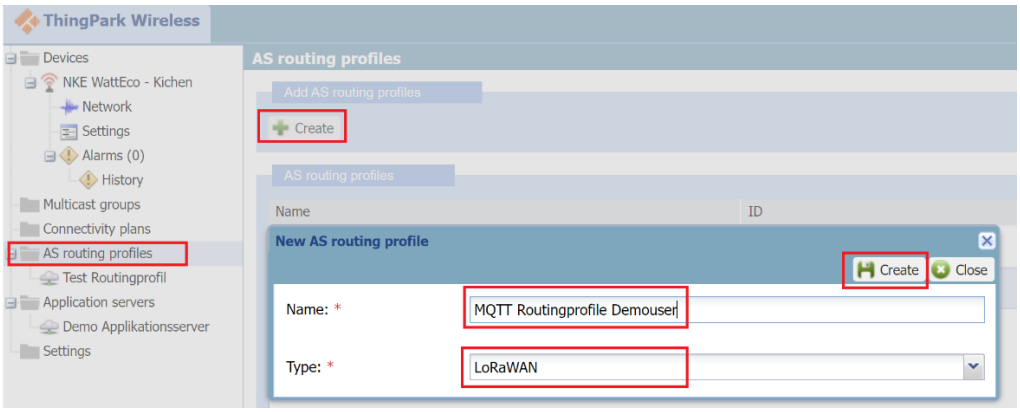

Abbildung 11: Erstellung Routingprofil

Im vorliegenden Beispiel wird ein **MQTT-Endpunkt** definiert. Hierfür wählt man zuerst einen passenden Namen für das Profile aus und setzt die **Type** auf „**LoRaWAN**“. Im Anschluss erscheint ein weiteres Fenster, wo die dazugehörigen Destinationen (Endpunkte müssen vom Internet aus erreichbar sein) spezifiziert werden. Neben dem Menüpunkt „**Supplier application server**“ – hier kann aus zwei von Wien Energie vordefinierten IoT Plattformen gewählt werden, muss die **Type** „**ThingPark X**“ und als **Destination** „**ThingPark X IOT-FLOW**“ ausgewählt werden.

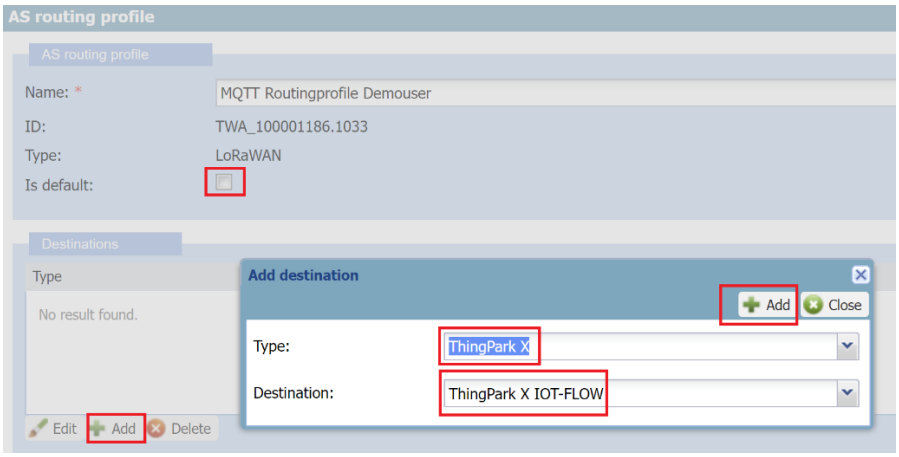

Abbildung 12: Definition Routingprofil

Nachdem das Routingprofil erstellt und aktiv ist (**Status Active**), können im **ThingPark X Interface** dazugehörige „**Flows/Connections**“ definiert werden, um die Datengegenstelle weiter zu spezifizieren.

TIPP: wenn die Einstellung „**Is default**“ angehakt ist, wird bei Anlegen eines jeden neuen Endgeräts das Routingprofil standardmäßig verwendet und muss nicht mehr extra im Device Manager auf Endkundengerät-Ebene ausgewählt werden.

2.2.6 Assoziation eines Routingprofils mit bestehenden Endkundengeräten

Jenes im vorherigen Kapitel erstellte Routingprofil (**TPX-Routingprofil**), muss im Anschluss mit etwaig bestehenden Endkundengeräten – bei denen dieses Profil bei Erstellung noch nicht hinterlegt ist – verknüpft werden. Hierzu ruft man die Endkundengeräte Übersicht im Device Manager auf und editiert das einzelne Endkundengerät, indem man auf das Stiftsymbol klickt.

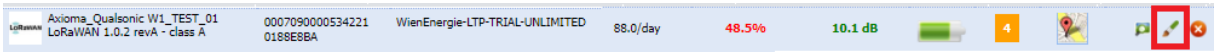

Abbildung 13: Endkundengeräte editieren

Danach öffnet sich ein neues Fenster, das spezifisch für das zu editierende Endkundengerät gilt.

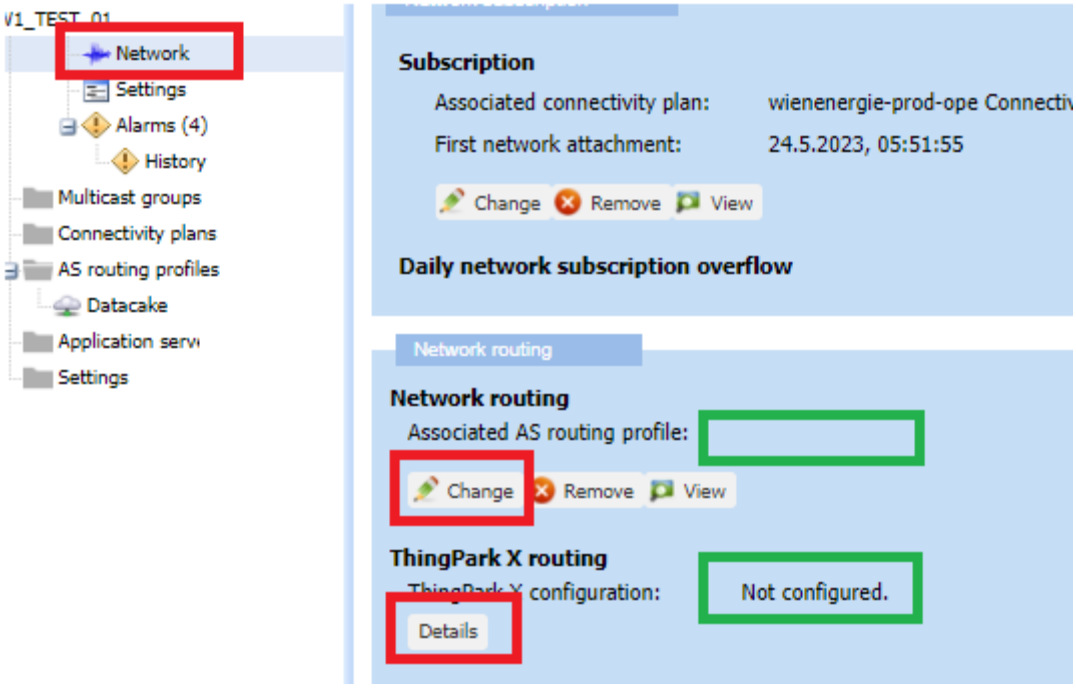

Abbildung 14: Routingprofil anzeigen

Unter dem Reiter „**Network**“ sieht man, dass aktuell kein Routingprofil (siehe **grüne** Felder) verknüpft wurde. Wie im vorherigen Kapitel erstellt, wählen wir nun das TPX-Routingprofil „**MQTT Routingprofile Demouser**“ aus, indem wir „**Change**“ auswählen, das Profil setzen und auf „**Save“** klicken.

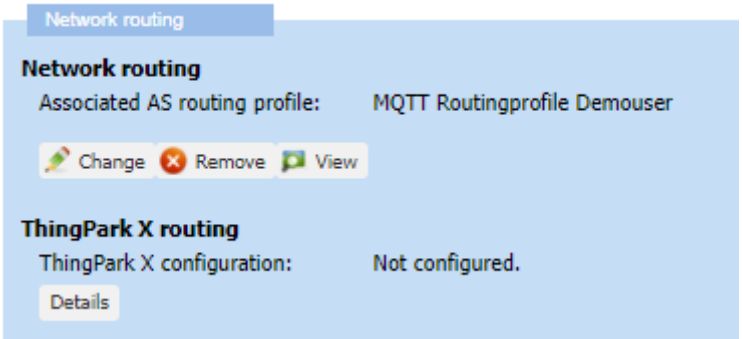

Abbildung 15: Routingprofil setzen

Abschließend muss unter dem Punkt „**ThingPark X routing**“ noch der im **ThingPark X IOT Flow** gewählte „**Tag**“ konfigurieren, um den richtigen Flow zu wählen. Siehe diesbezüglich **Kapitel 2.3.1**.

In Beispiel wird der Tag „**demotag**“ inklusive eines beliebigen **Ports** (von 0 bis 255) gesetzt. Das Port dient lediglich für administrative Zwecke und kann frei gewählt werden. Es können mehrere unterschiedliche Tags und dazugehörige Ports verwendet werden.

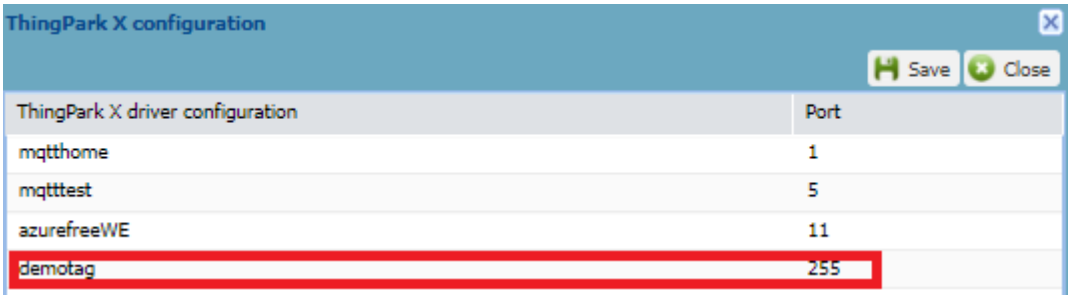

Abbildung 16: Routingprofil Tag setzen

Mit „**Save**“ speichert man die Einstellungen. Beim nächsten Uplink des Endkundengeräts wird das TPX-Routingprofil ausgewählt und die Daten zur gewünschten Endstelle gesendet.

2.3 ThingPark X Interface

ThingPark X (**TPX**) dient zur Definition der Datenübergabepunkte an externe Kundensysteme und ist über ein eigenständiges Web-Service erreichbar. Die Applikation bietet zudem die Möglichkeit an, Nutzdaten aus den verschlüsselten Endgerätedaten lesbar zu machen (**Payload Decoding**) sowie die gewünschte Datenstruktur zu definieren.

Der Zugriff erfolgt mittels Administratorbenutzer des jeweiligen Kunden über die genannte URL – **siehe Kapitel 1.1**. Nach erfolgreicher Authentifizierung ist das **TPX-Dashboard** ersichtlich.

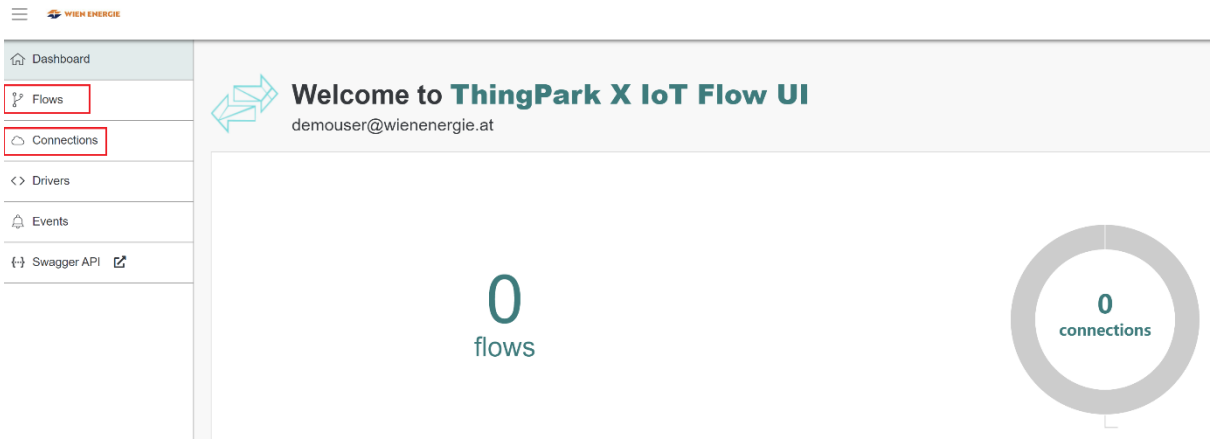

Abbildung 17: ThingPark X Dashboard

Für die Weiterleitung von Nutzdaten müssen ein/mehrere „**Flow(s)**“ und eine/mehrere „**Connection(s)**“ definiert werden, um Daten an externe Drittsysteme zu senden. Unter dem Punkt „**Drivers**“ wird die Möglichkeit zum Payload-Decoding angeboten, wobei aktuell (**Stand: 11.07.2023**) bereits für mehr als 462 unterschiedliche Endgerätetypen ein Payload-Decoder hinterlegt ist. Kunden haben zudem die Möglichkeit, eigene Payload-Decoder unter dem Punkt Drivers zu programmieren.

2.3.1 Datenflow und Datenconnection erstellen

Ein **Datenflow** identifiziert Endkundengeräte anhand bestimmter Kriterien. Dies können die eindeutigen DevEUIs, oder auch spezifische Kundenbezeichnungen („**Tags**“), sein. **Connections** hingegen spezifizieren zumeist das Protokoll oder die Applikation der Gegenstelle (zB. MQTT, http(s) oder Microsoft Azure). Flows und Connection können sowohl einzeln als auch getrennt voneinander erstellt werden.

In unserem Beispiel (Neuanlage eines Flow und einer Connection) können beide mit nur einem Wizard erstellt werden, indem man auf „**ADD FLOW**“ klickt.

Nachdem der Wizard gestartet wurde, definiert man eine beliebige Bezeichnung für den Flow. Nach Eingabe der Parameter und dem Klick auf „**Continue**“ wird die Identifikation der hierfür notwendigen Endkundengeräte gefordert.

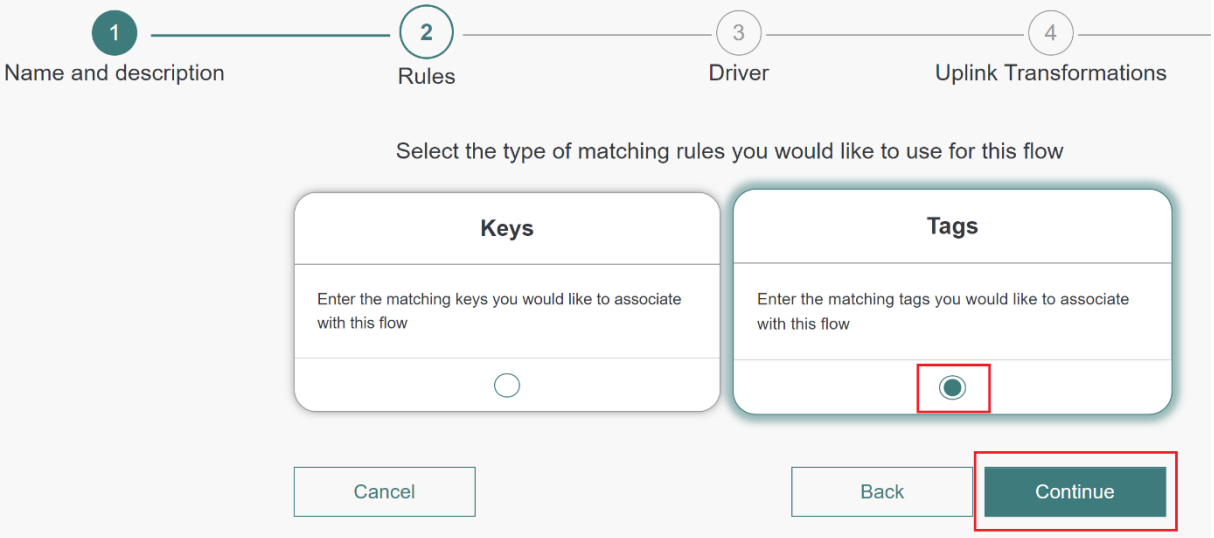

Abbildung 18: TPX Flow Tags definieren

In unserem Beispiel wollen wir alle Endkundengeräte einer bestimmten **Gruppe/Logik/Zieldefinition** mit Hilfe von „**Tags**“ identifizieren. Es wird hierfür der Tag „**demotag**“ definiert.

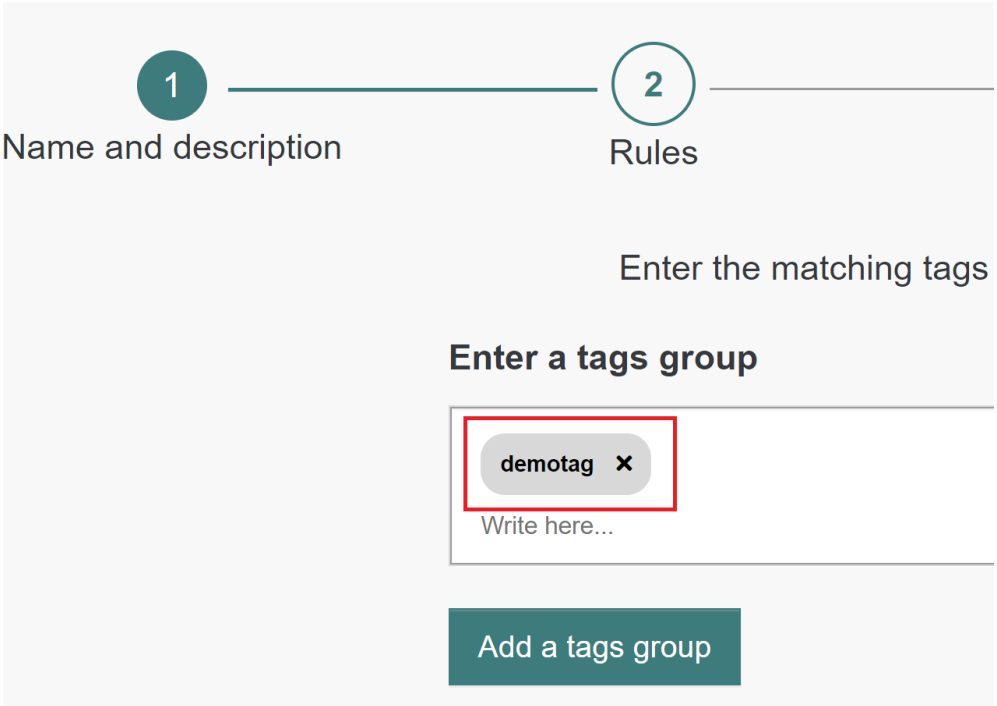

Abbildung 19: TPX Flow tag „demotag“

Als nächstes werden wir gefragt, wie die Identifikation und Zuweisung von Endkundengerätetypen zu möglichem Payload-Decoder (**Driver**) erfolgen soll. Im vorliegenden Fall belassen wir die Identifikation automatisiert, da für jedes am Netzwerkserver bekannte Endkundengerät mit Hilfe von Hersteller und Type ein Driver hinterlegt ist. Wir belassen die Option „**Automatic**“ ausgewählt, um den LPWAN Driver automatisch vom System zu nutzen.

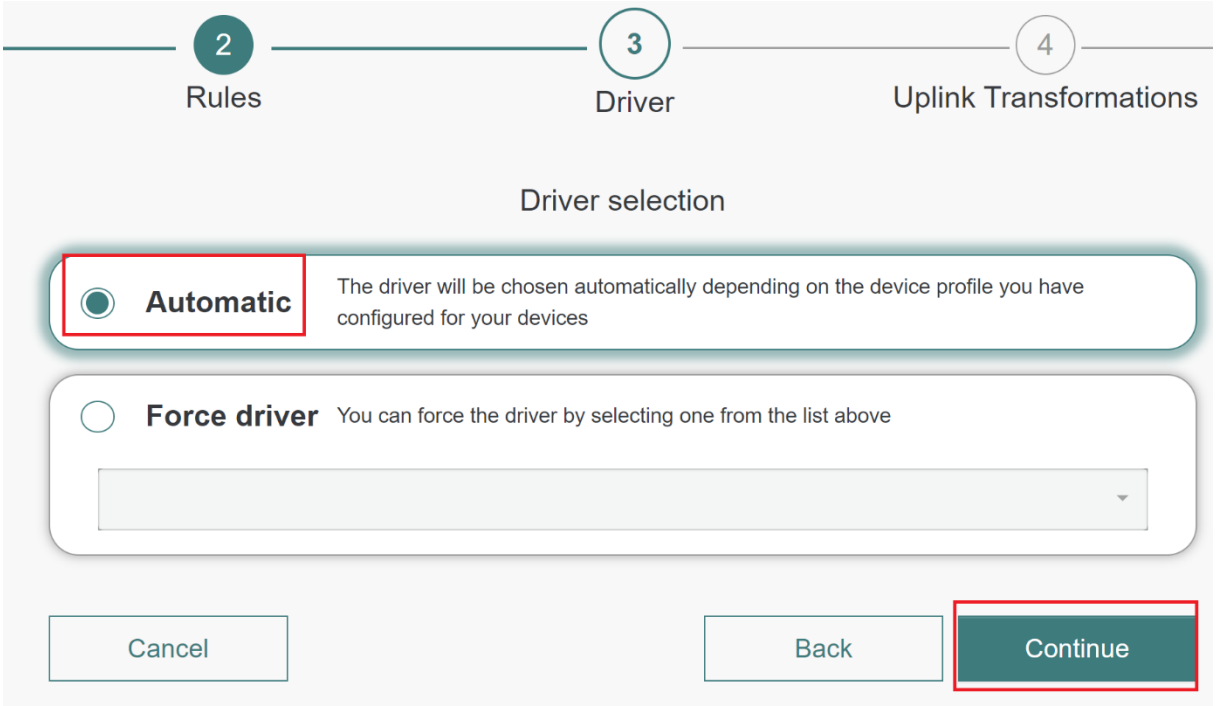

Abbildung 20: TPX Driver Identifikation

Danach besteht die Möglichkeit, die Nutzdaten der Endkundengeräte über die Schnittstelle in ein bestimmtes Format bzw. in eine bestimmte Reihenfolge zu bringen, indem man die Daten mittels „**Uplink Transformations**“ umwandelt.

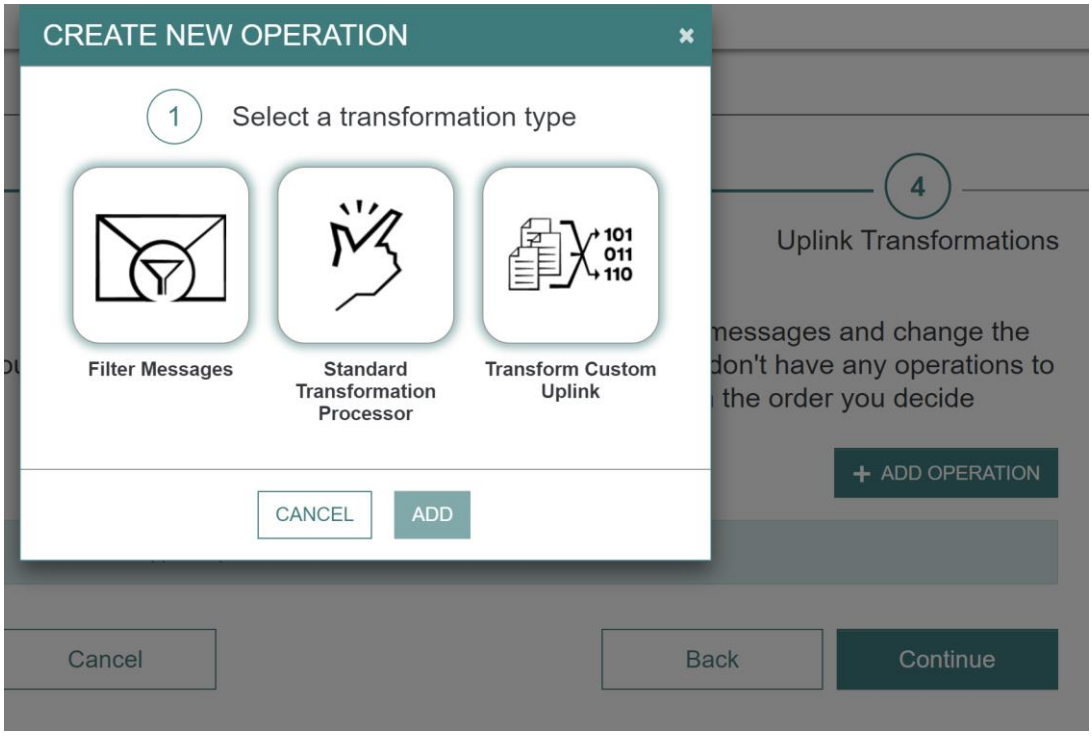

Abbildung 21: TPX Uplink Transformation

Die Funktion „**Uplink-Transformation**“ bedarf eines detaillierteren Verständnisses für die spezifische Nachrichtenverarbeitung bzw. dessen Syntax (zB. JSLT, JSONATA oä.). In der Praxis hat sich gezeigt, dass eine Anpassung der Nutzdaten Reihenfolge zumeist (erst) am externen Drittsystem Sinn ergibt. Dies ist jedoch sehr Use-Case spezifisch und kann von Fall zu Fall stark variieren. Im nachfolgenden

Beispiel führen wir keine Umwandlung der Endgerätenutzdaten durch und klicken daher auf weiter – (ohne Transformation).

Abschließend wird innerhalb des Wizards noch die gewünschte „**Connection**“ definiert. In unserem Fall ist unsere Gegenstelle – das externe **Datenziel/Protokoll** – ein **MQTT-Broker**. Hierfür müssen im nächsten Fenster noch die Details (Benutzername/Password, Authentifizierung-Modus etc.) spezifiziert werden, um eine erfolgreiche Verbindung zwischen LPWAN Netzwerkserver und dem MQTT-Broker aufzubauen.

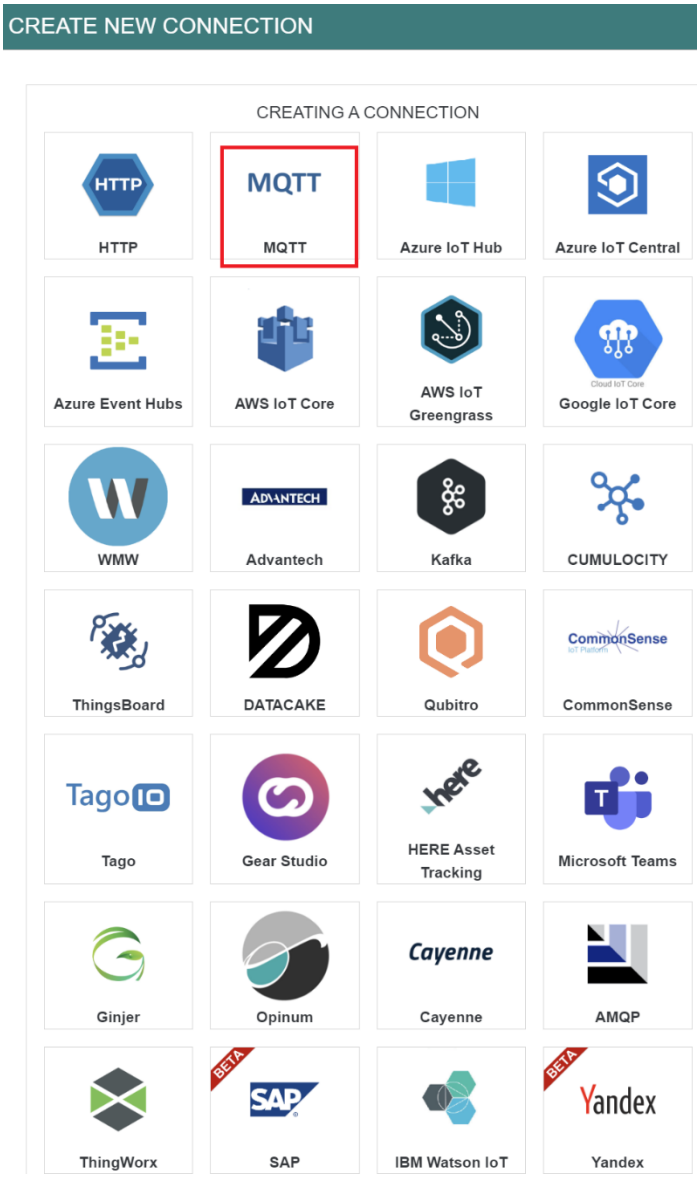

Abbildung 22: TPX-Connection Auswahl

Die einzustellenden Optionen sind für jede Connection unterschiedlich und können von Use-Case zu Use-Case oder Connection stark variieren.

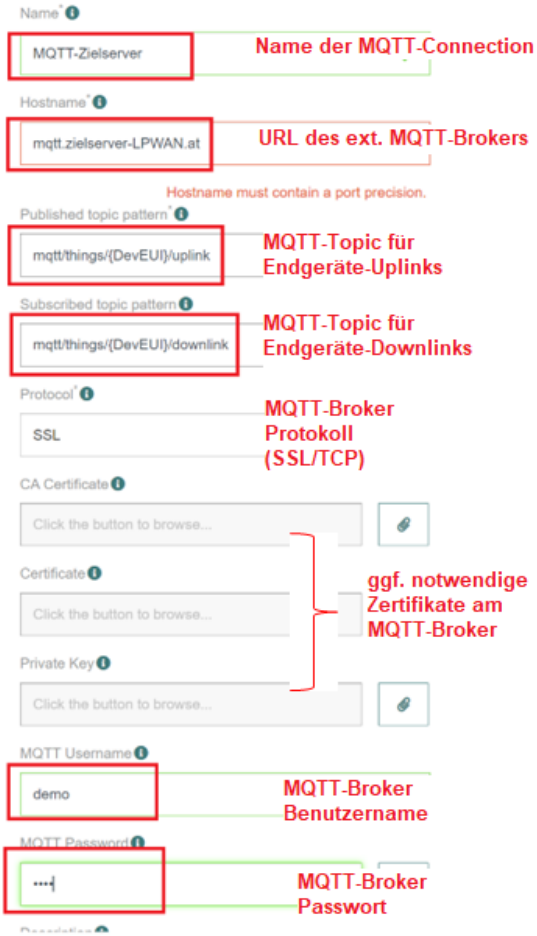

Abbildung 23: MQTT-Connection Details

Im dargestellten Beispiel wurde für die MQTT-Connection ein Mindestmaß an Optionen definiert (Musskriterien), die bei der Anmeldung am externen MQTT-Broker benötigt werden. Je nach verwendetem MQTT-Broker, können bzw. müssen weitere Optionen (zB. spezifische Zertifikate) eingestellt werden.

TIPP: Wien Energie bietet ihren Kunden einen MQTT-Broker mit einem kundenspezifischen MQTT-Topic (**Beispiel für Topic:** „**KundeXY/LPWAN**“ inkl. Lese und Schreiberechte zur Verfügung. Sollten Sie daran Interesse haben, kontaktieren Sie uns unter iot@wienenergie.at.

2.3.2 Logeinträge zu Connections

Möchte man verifizieren, ob eine Verbindung erfolgreich aufgebaut wurde bzw. welches Problem es zuletzt gab, so kann das „**Event**“ Menü auf der linken Seite aufgerufen werden.

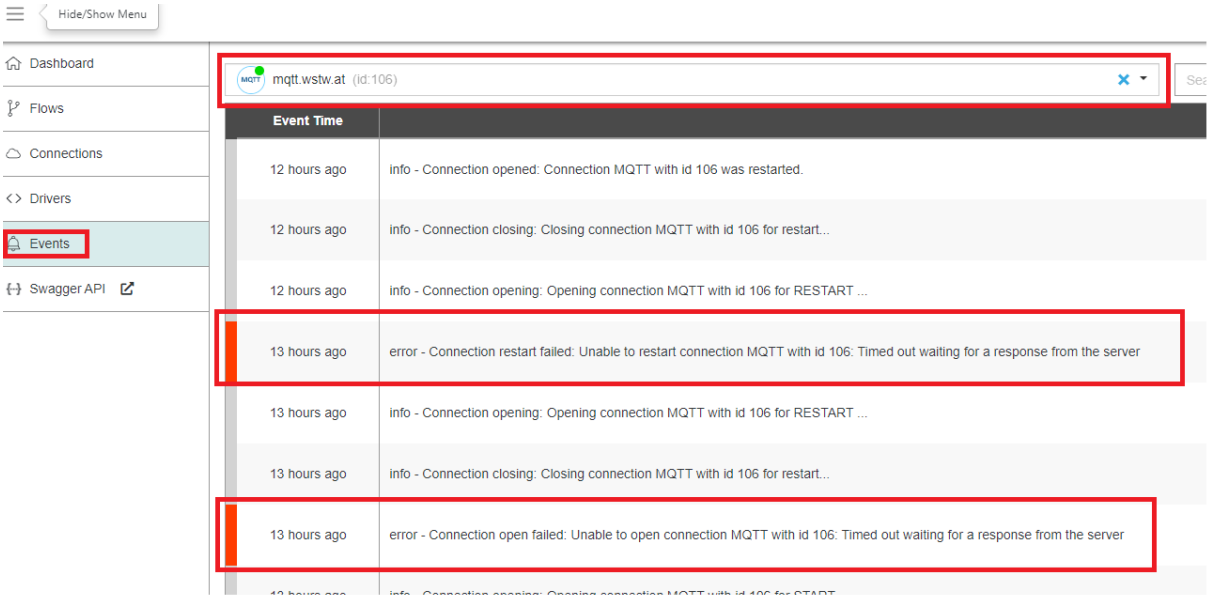

Abbildung 24: TPX-Eventübersicht

Zwecks einfacherer Übersicht kann in den Events auf eine spezifische Connection gefiltert werden. In unserem Beispiel werden nur Events für die MQTT-Connection („**mqtt.wstw.at**“) angezeigt. In der Abbildung ist ersichtlich, dass es vor 13 Stunden (zum Zeitpunkt des Aufrufs des Eventtabs) kurze Aussetzer bei der Verbindung gab, wobei sich die Verbindung kurz darauf neu gestartet hat und erfolgreich verbunden wurde (**Connection opened**).

2.3.3 Downlinks an Endkundengeräte via MQTT

Neben Daten von Endkundengeräten zu erhalten, bietet die TPX-Applikation die komfortable Möglichkeit an, Downlink-Nachrichten an eine Vielzahl von Endgeräten via MQTT-Protokoll zu senden. Hierfür muss in der zuvor definierten MQTT-Connection - siehe **Abbildung 22** - ein Topic für Downlink-Nachrichten definiert worden sein.

Das im Beispiel gewählte Topic „**mqtt/things/{DevEUI}/downlink**“ ist beliebig wählbar und besitzt aktuell eine Variable (default bei der Erstellung) mit der Bezeichnung „**{DevEUI}**“. Diese Variable wird im Downlink-Topic nicht empfohlen, da der Sensor mit seiner eindeutigen **DevEUI** im Nutzdatenfeld (Payload) identifiziert wird.

Es würde demnach ausreichen, als Downlink-Topic beispielhaft „**mqtt/thing/downlink**“ zu wählen.

Die zu sendende Payload an den MQTT-Broker hat zumindest folgende JSON-Struktur und Parameter zu beinhalten:

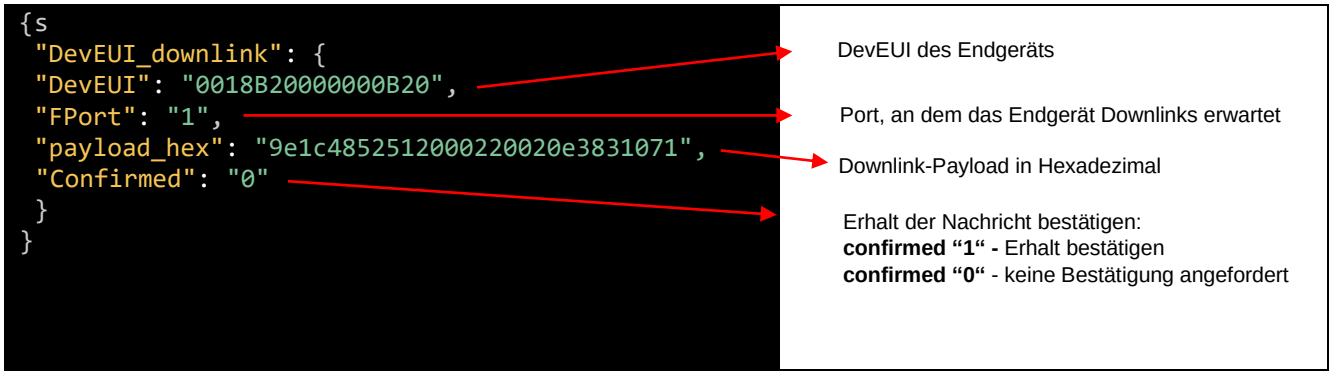

Tabelle 2: Downlink-Nachricht MUSS-Kriterien

Optional können weitere Parameter mitgegeben werden, beispielhafte Anführung:

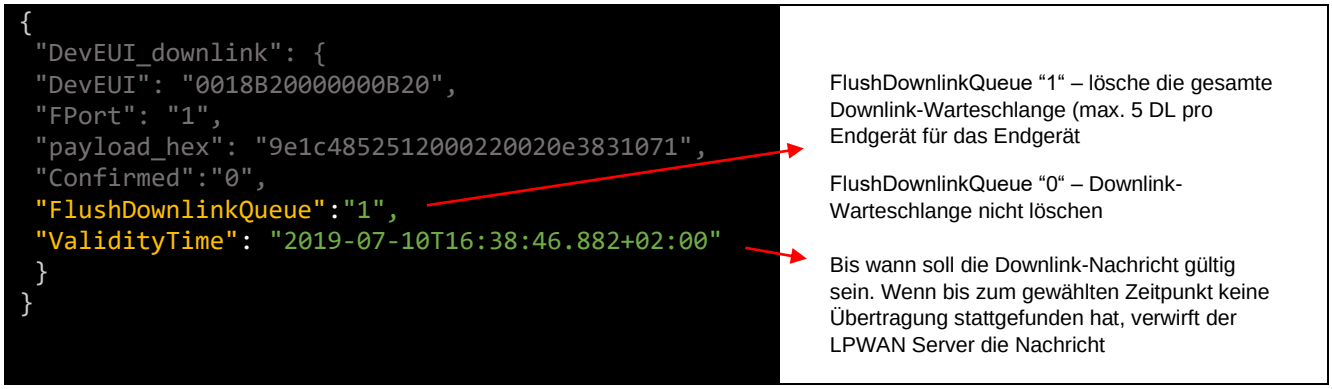

Tabelle 3: Downlink-Nachricht Optionale-Kriterien

Die Darstellung der optionalen Parameter ist in der Abbildung nicht vollständig und repräsentiert lediglich oft genutzte Optionen. Eine komplette Liste mit allen möglichen Parametern befindet sich im Anhang – **siehe** „**Downlink-Nachricht Parameter**".

TIPP: Beachten Sie stets die JSON-konforme Formatierung ihrer Payload, indem sie „Klammern", „Beistriche" als auch „Anführungszeichen" richtig positionieren. Hierfür gibt es im Internet unterschiedliche Tools, um die Formatierung zu prüfen. Beispielhaft sind die Services wie von https://jsonformatter.curiousconcept.com angeboten.

2.4 LPWAN Wireless Logger

Der LPWAN Wireless Logger ist die Applikation zur Einsicht von LPWAN Funkpaketen von Endkundengeräten im Wien Energie LPWAN Netzwerk. Der jeweilige Endkunde kann in seiner LPWAN Wireless Logger Applikation nur die Funknetzpakete seiner eigenen (aktiven) LPWAN Endkundengeräte einsehen. Auf Endkundenbenutzerebene reicht zum Anzeigen der Pakete eine Leseberechtigung aus.

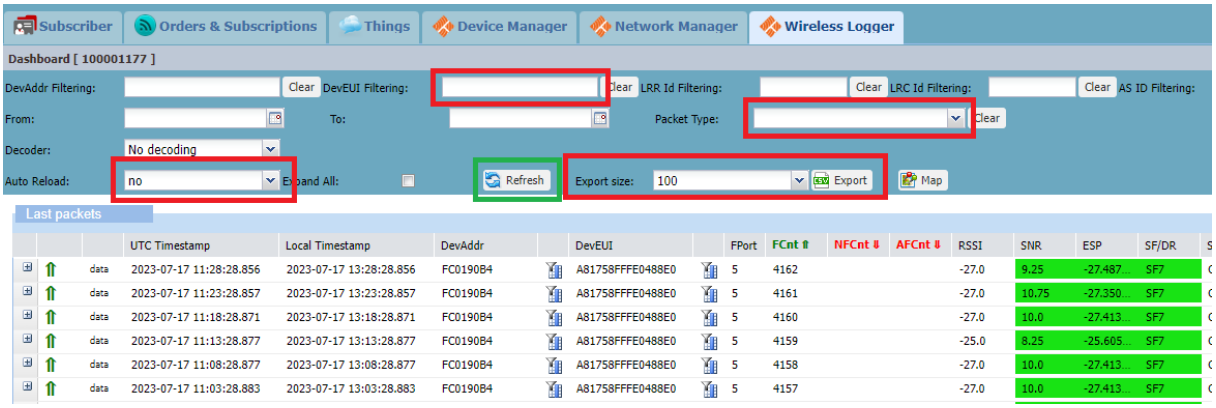

Abbildung 25: Wireless Logger Übersicht

Zum Aktualisieren von Daten wird der **grüne** Knopf „Refresh“ geklickt. Möchte man die Informationen einschränken, so lässt sich dies auf unterschiedlichste Art und Weise realisieren.

Geläufige Filter- bzw. Einstellmöglichkeiten sind zB.:

DevEUI Filtering	Eingabe in Hexadezimal	... Informationen für einen spezifischen Sensor
Packet Type	Auswahlfeld/Drop-Down	… Filter für Join, Uplink, Downlink etc. Nachrichten
Auto Reload	No/10s/20s/30s..	… automatischer Reload alle XX Sekunden

Tabelle 4: Wireless Logger Filter

Zudem lassen sich sämtliche (auch filterspezifischen) Daten mittels einfacher Funktion (Exportfeld) als CSV-Datei exportieren. Hierbei ist die maximale Anzahl auf 500 Zeilen pro Export begrenzt.

Wenn es Verbindungs- oder Endgeräteprobleme im LPWAN Funknetzwerk gibt und Sie Informationen zur Datenübertragung benötigen, ist der LPWAN Wireless Logger Ihre erste Anlaufstelle, um qualifizierte Aussagen treffen zu können und die Probleme weiter einzugrenzen.

TIPP: mehrere gleichzeitig gesetzte Suchfilter werden als logisches **UND** verstanden und grenzen die Suche weiter ein. Mehrere Daten innerhalb eines Suchfeldes (zB. DevEUI) können mit einem Komma (**,**) getrennt angeführt werden. Wildcards werden bei der Suchfunktion nicht unterstützt.

2.4.1 Verifikation von Endgeräte-Verbindungen (Join + Join-Accept)

Um in zyklischen Abständen Nutzdaten über das Wien Energie LPWAN Funknetzwerk senden zu können, müssen Endkundengeräte erfolgreich im LPWAN Funknetzwerk der Wien Energie autorisiert sein. Hierfür ist es unabdingbar, dass nach Einrichtung des Kundengeräts – siehe LPWAN Endkundengeräte erstellen – durch das Endkundengerät selbst ein erster Kontakt mit dem Funknetzwerk (Join-Versuch) aufgebaut wurde. Auf das Join-Paket inkl. Antwortpaket kann mit einem spezifischen Filter im Wireless Logger unter dem Punkt „**Packet Type**“ – **Uplink (Join)** und **Downlink Unicast (Join)** sowie „**DevEUI**“ gefiltert werden.

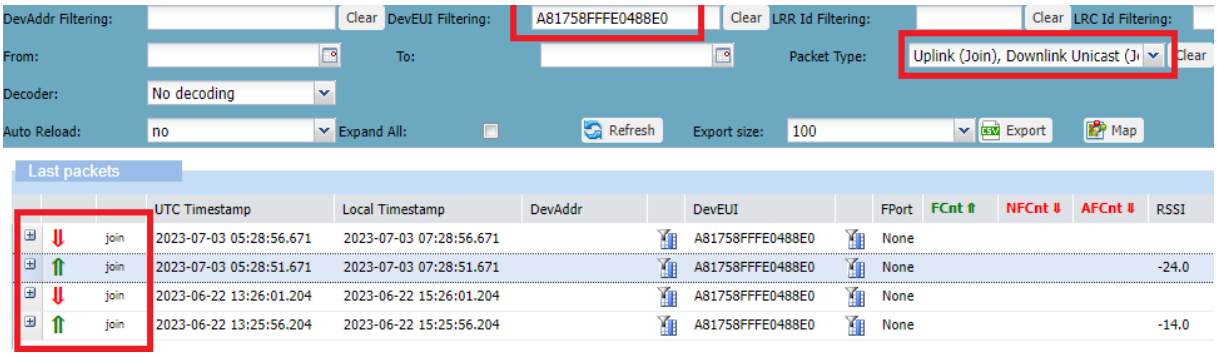

Abbildung 26: Join-Request und Join-Accept

Der Sensor hat (zu zwei unterschiedlichen Zeiten) Join-Requests gesandt, die vom LPWAN Netzwerkserver wenige Sekunden danach beantwortet wurden. Möchte man sich diese Pakete im Detail ansehen, so klickt man auf der linken Seite auf die „**+**“ Symbole. Es erweitern sich danach die Pakete mit Detailinformationen.

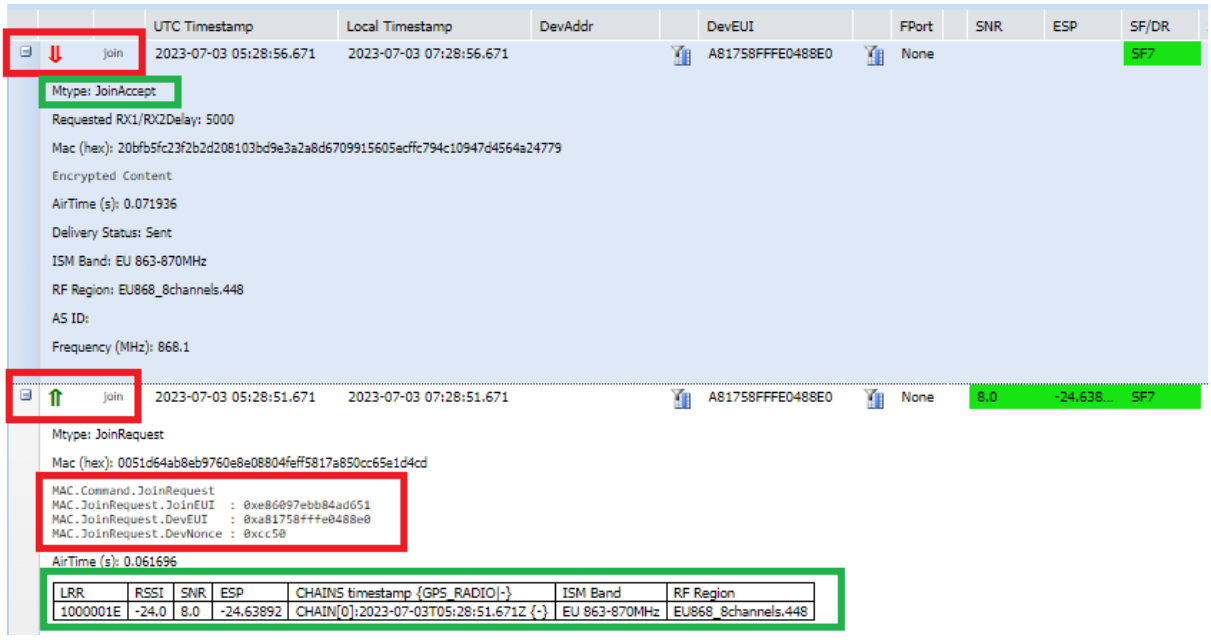

Abbildung 27: Join-Request und Join-Accept im Detail

Im ersten Paket (**grüner** Pfeil – **siehe Abbildung 27**) ist der Join-Request mitsamt dazugehörigen Informationen (DevEUI, AppEui(JoinEUI)) ersichtlich. Im grünen Feld ist ersichtlich, wie viele und welche Gateways das Datenpaket gesehen/weitergeleitet haben. Im aktuellen Beispiel hat ein Gateway das Paket empfangen und an den LPWAN Device Manager weitergeleitet. Zudem sind weitere Funknetz-Verbindungsparameter (Spreading Factor (SF), Signal to Noise Ratio (SNR) udgl.) ersichtlich.

Im Antwortpaket (**roter** Pfeil – **siehe Abbildung 27**) wurde der Join-Request vom Netzwerkserver erfolgreich beantwortet. Dies ist unter dem Punkt „**Mtype: Join Accept**“ ersichtlich. Nachdem ein erfolgreicher Join stattgefunden hat, ist im nächsten „**Uplink (Data only)**“ Paket eine „**DevAddr**“ (Geräteadresse innerhalb des LPWAN Netzwerks) beim Device ersichtlich.

2.4.2 Verifikation von Uplink und Downlink Datenpaketen von/an Endkundengeräte

Möchte man sich jegliche **Uplink-Datenpakete** von Endkundengeräten anzeigen lassen, so können diese spezifisch im Wireless Logger gefiltert werden. Hierzu empfiehlt es sich, sämtliche „**Uplink ***“ Packet Typen auszuwählen.

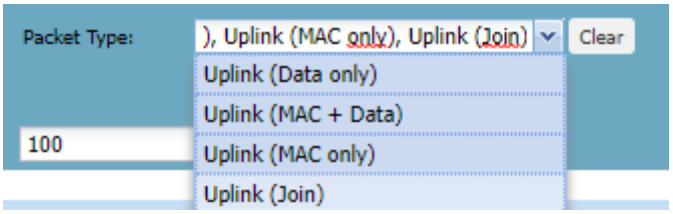

Abbildung 28: Uplink-Paket Filterung

Nach erneutem Klick auf „**Refresh**“ sieht man die (Uplink) Datenpakete des gewählten Filters. Nachfolgend wird ein Uplink-Paket mit Dateninformationen (**Data** | Payload) genauer dargestellt.

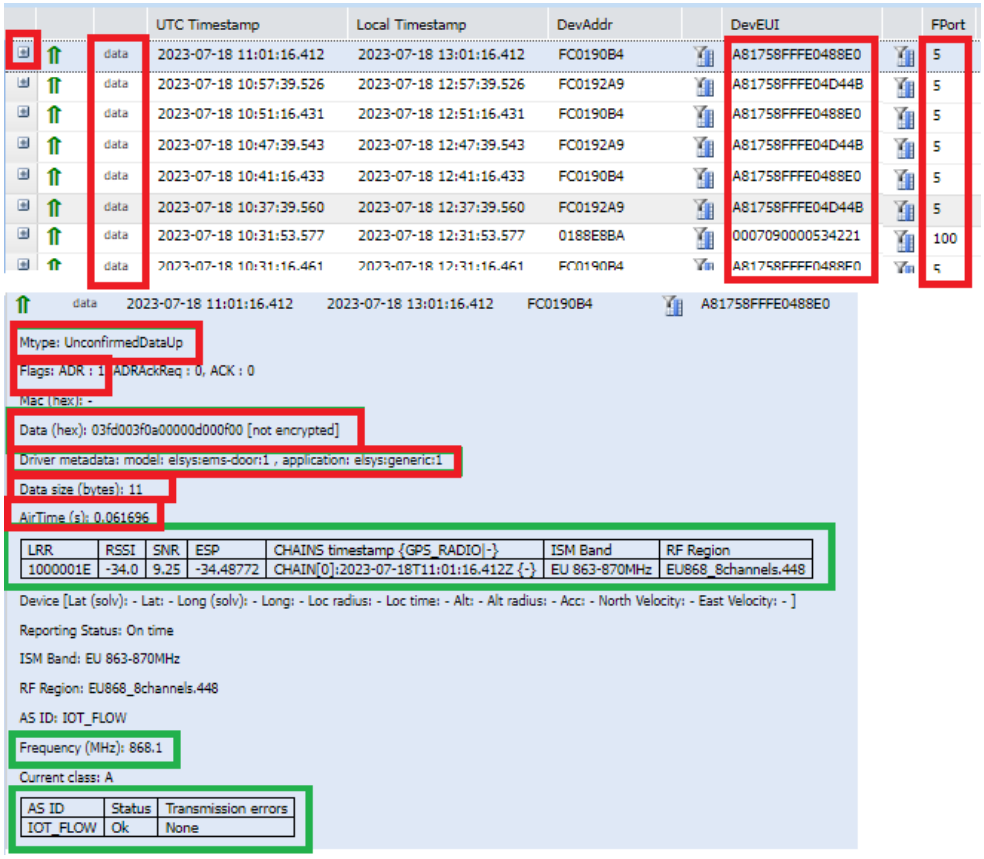

Abbildung 29: Uplink-Paket Data Payload

In **Abbildung 29** sind die unterschiedlichsten Informationen der Datenübertragung graphisch aufgelistet. Neben Endgeräteinformationen, die unmittelbar mit dem Endgerät in Verbindung gebracht werden können (**rot**), befinden sich auch Metainformationen (**grün**) zur Übertragung bzw. der LPWAN Netzwerkinfrastruktur in der Ansicht.

Ein Klick auf das **„+“** Symbol erweitert pro Datenpaket die Ansicht und führt zu den gewünschten Informationen. Folgende Details finden für gewöhnlich die meiste Verwendung:

DevEUI	Eindeutige Endgeräte ID
FPort	Endgeräte Übertragungsport
Mtype: UnconfirmedUp	Pakettype
Flags: ADR	Adaptive Datenrate – dynamische Optimierung von Überrtragungen im Sinne der Sendezeit/des Energieverbrauchs **0** … **Aus** **1** … **Ein**
Data (hex)	Nutzdaten in Hexadezimal
Driver metadata:model:application	Gewählter Driver (TPX) – hier automatisch gewählt
Data size (bytes)	Paketgröße in bytes
AirTime (s)	Zeit für die Übertragung im LPWAN Netzwerk
LRR	Gateway-ID / Anzahl der gesehenen Gateways
Frequency (Mhz)	Genutzte Übertragungsfrequenz
AS_ID | Status | Transmission errors	Genutzte Applikation / Status zur Übertragung / Fehler

Tabelle 5: Uplink-Paket Details

Analog zur Verifikation der Uplink-Datenpakete, können auch bereits übermittelnde **Downlink-Pakete** an Endkundengeräte dargestellt werden. Hierzu empfiehlt es sich, sämtliche „**Downlink *“** Packet Typen auszuwählen. Aktuell ist es nicht möglich, sich in der Warteschlange befindliche Downlink-Nachrichten anzuzeigen. Diese können erst eingesehen werden, nachdem Sie über den Netzwerkserver an das Endkundengerät gesandt wurden.

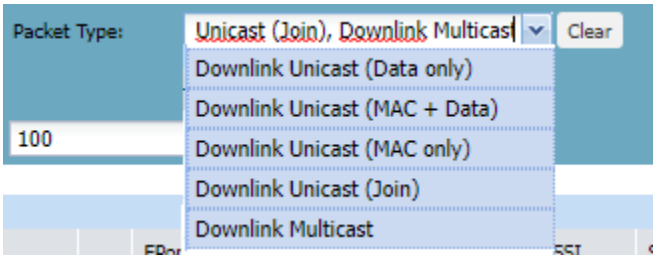

Abbildung 30: Downlink-Paket Filterung

Nach erneutem Klick auf „**Refresh**“ sieht man die (Uplink) Datenpakete des gewählten Filters. Nachfolgend wird ein Uplink-Paket mit Dateninformationen (**MAC** | Payload) genauer dargestellt.

Abbildung 31: Downlink-Paket MAC Payload

Ebenso wie das Uplink-Paket enthält das Downlink-Paket verwandte Informationen. Im vorliegenden Beispiel ist eine Downlink-Nachricht vom LPWAN Server an ein ausgewähltes Endgerät ersichtlich, wo die MAC-Nutzdaten (in Hexadezimal) vom Server in lesbaren Code umgewandelt werden, da es sich

um einen bekannten MAC-Command vom LPWAN Server handelt. Im Detail ist dies ein „**LinkADRReq**“ vom Server zum Endgerät, der das Endgerät anweist, seine Datenrate, Sendeleistung, Kanal oder Sendewiederholungsrate zu adaptieren.

2.4.3 Verifikation von Datenübertragungen an externe Kundensysteme

Etwaige Fehler bei der Weiterleitung der Nutzdaten an ein externes Drittsystem können zudem unter dem Punkt „**AS_ID | Status | Transmission errors“** schnell identifiziert werden.

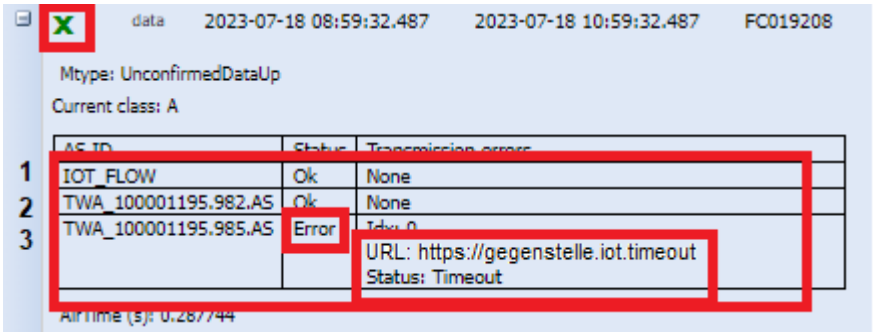

Abbildung 32: Fehler bei der Datenübertragung

Der **Abbildung 32** kann entnommen werden, dass das Endkundengerät seine Daten an drei (**3**) unterschiedliche Endstellen gesandt hat. Bei den ersten beiden „**AS_ID**“ kam nach der Übertragung eine Bestätigung zurück, weshalb der LPWAN Server die Übertragung als in Ordnung „OK“ klassifiziert. Bei der letzten Übertragung wurde im vorliegenden Beispiel eine falsche URL eingetragen, die eine Fehlermeldung vom Webserver zurückgab und als Fehlerbehaftet „**Error**“ angezeigt wird.

Sollte nur ein „**AS_ID**“ Flow konfiguriert sein oder sollte ein Fehler bei der Übertragung bei allen drei Endstellen aufgetreten sein, so wäre kein grünes, sondern ein rotes „**X**“ nehmen dem Data-Feld ersichtlich.

2.5 API-Schnittstelle

LPWAN Kunden besitzen über eine zentrale API-Schnittstelle die Möglichkeit, sämtliche in der Weboberfläche durchgeführten (händischen) Änderungen mittels Drittsystemen an den LPWAN Server zu senden. Hierbei handelt es sich um eine **REST-API** die GET / POST / PUT / DELETE Befehle unterstützt. Neben dem Setzen und Verändern von Parametern der **Device Manager** Applikation, können auch Einstellungen von **ThingPark X** mit der API durchgeführt werden.

Die API gliedert sich in zwei Hauptmodule:

DX Admin API	Interface, um einen API-Schlüssel zu generieren (Authentifizierungsebene)
DX Core API	Interface zum Austausch für Konfigurationsdaten (Konfigurationsebene)

Tabelle 6: API-Module

Nachfolgend werden exemplarisch einzelne Schritte zur Verwendung der Schnittstelle erklärt und mit Hilfe von Beispielen dargestellt.

2.5.1 Authentifizierung auf der Schnittstelle „Dx-Admin API“

Um mit der API-Schnittstelle kommunizieren und Konfigurationsparameter austauschen zu können, müssen Endkunden mit ihrem Administratorbenutzer und Passwort einen zeitlich (un)begrenzten API-Schlüssel generieren. Hierfür öffnet man die URL der zentralen Schnittstelle – **siehe Tabelle 1**.

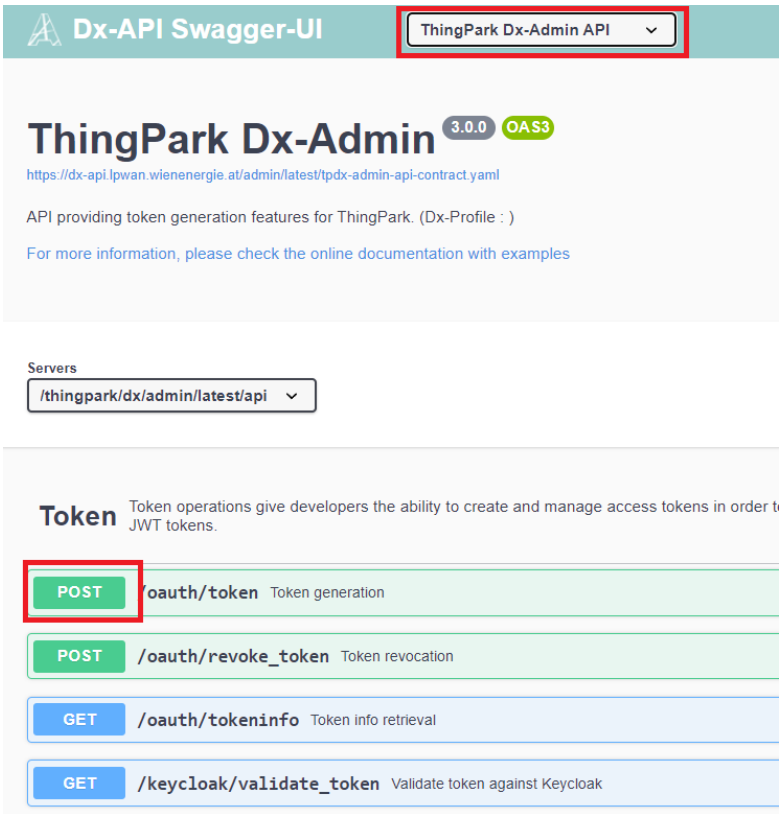

Abbildung 33: API Post

Um einen API-Schlüssel zu generieren, wählt man „**ThingPark DX-Admin API**“ aus und klickt für die Erstellung eines neuen, oder Verlängerung eines bereits bestehenden Schlüssels, auf den Tab „**POST**“.

Danach werden Felder zwecks Eingabe von kundenspezifischen Angaben abgefragt, die vom Endkunden befüllt werden müssen.

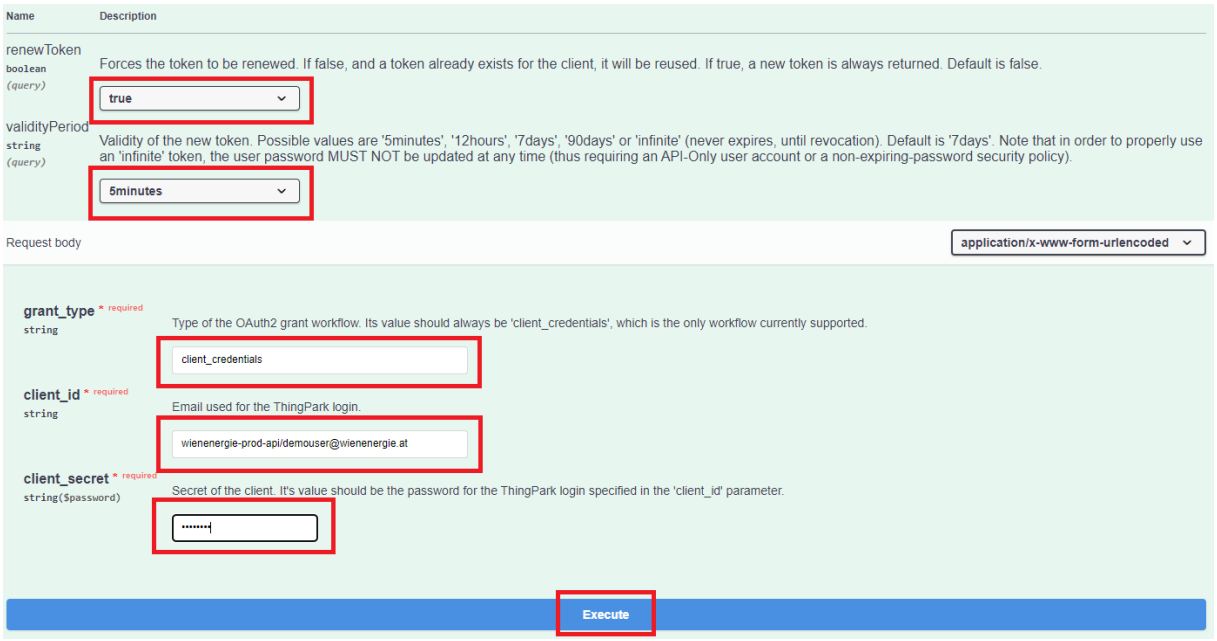

Abbildung 34: API Post Detail

Die unterschiedlichen Parameter sind hierbei wie folgt zu verstehen:

renewToken	Soll ein bestehender Schlüssel erneuert oder ein bestehender weiter verwendet werden (Beispiel: true)
validityPerion	(un)begrenzter Gültigkeitszeitraum des API-Schlüssels
grant_type	Funktion – „**client_credentials**“ muss ausgefüllt sein
client_id	Authentifizierung zur Erstellung eines Schlüssels: **„wienenergie-pro-api/“ muss** vor Admin Benutzer vorangestellt werden
client_secret	Passwort des Admin Benutzers

Tabelle 7: API Post Optionen

Nach Bestätigung mit „**Execute**“ wird der API-Schlüssel angefordert und im nächsten Feld mittels Rückmeldung bestätigt. Ebenso werden etwaige Fehlermeldungen (zB. fehlerhafte Authentifizierung) in der Antwort mit ausgegeben.

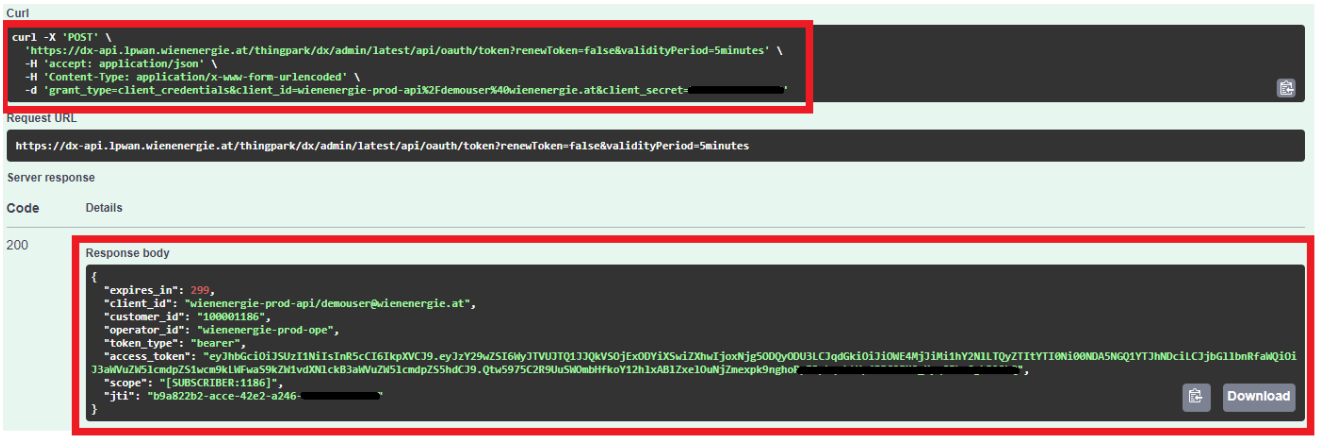

Abbildung 35: API Post Rückmeldung

In **Abbildung 35** ist die Rückmeldung der API ersichtlich. Der „**access_token**“ ist der API-Schlüssel, der für die Dauer - siehe „**expires_in**“ - in Sekunden zur Verfügung steht. Ebenso wird der dazugehörige CURL-Befehl als Beispiel mit ausgegeben, um den Befehl auch via Command-line von einem externen Drittsystem aus zu senden.

2.5.2 Verwendung der Schnittstelle „Dx-Core API“

Nachdem der API-Schlüssel erstellt wurde, kann mittels REST-Befehlen mit dem System kommuniziert werden. Hierfür kann man direkt aus dem Web-Browser (erfolgreich getestet mit Google Chrome Version 114.0.5735.199) auf die „**ThingPark DX-Core API**“ zugreifen, indem man die Schnittstelle wechselt. Alternativ steht auch der Zugriff mittels **CURL-Befehle** zur Verfügung.

Abbildung 36: Wechsel zu DX-Core API

Mit Hilfe der “**DX-Core API**” lassen sich sowohl Konfigurations- als auch Statusparameter verifizieren, setzen bzw. löschen. Eine ausführliche Beschreibung sämtlicher DX-Core API Funktionalitäten kann unter dem **Link** bei dem Punkt „**Dokumentation der API“** in der **Tabelle 1** entnommen werden.

Nachfolgend wird die Nutzung der API-Schnittstelle mit dem Browser noch anhand eines Beispiels nähergebracht.

2.5.3 Abfragen von Endgeräte-Informationen über die API-Schnittstelle

Beispielhaft können mit der API detaillierte Informationen zu LPWAN Endkundengeräten ausgelesen oder auch Endgeräte angelegt bzw. gelöscht werden.

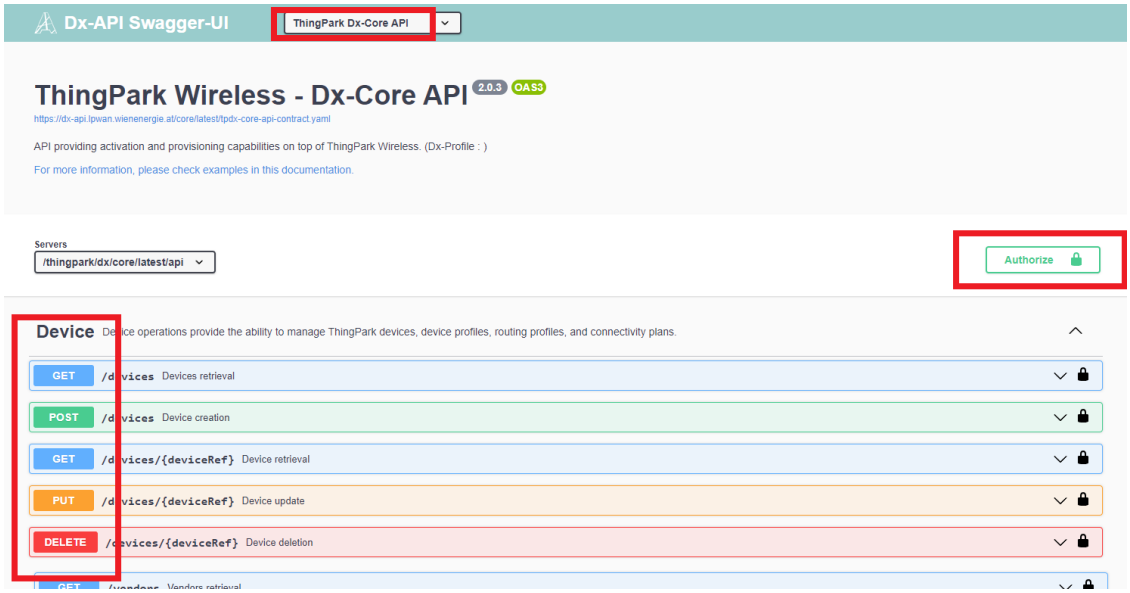

Abbildung 37: Dx-Core API Endgeräte

Hierzu scrollt man zur Überschrift „**Device**“ und wählt den gewünschten Befehlt aus. In unserem Beispiel wollen wir uns sämtliche LPWAN Endkundengeräte von unserem Bereich ansehen. Ein Klick auf „**GET**“ öffnet die entsprechende Auswahlmaske, die weiter spezifiziert werden kann.

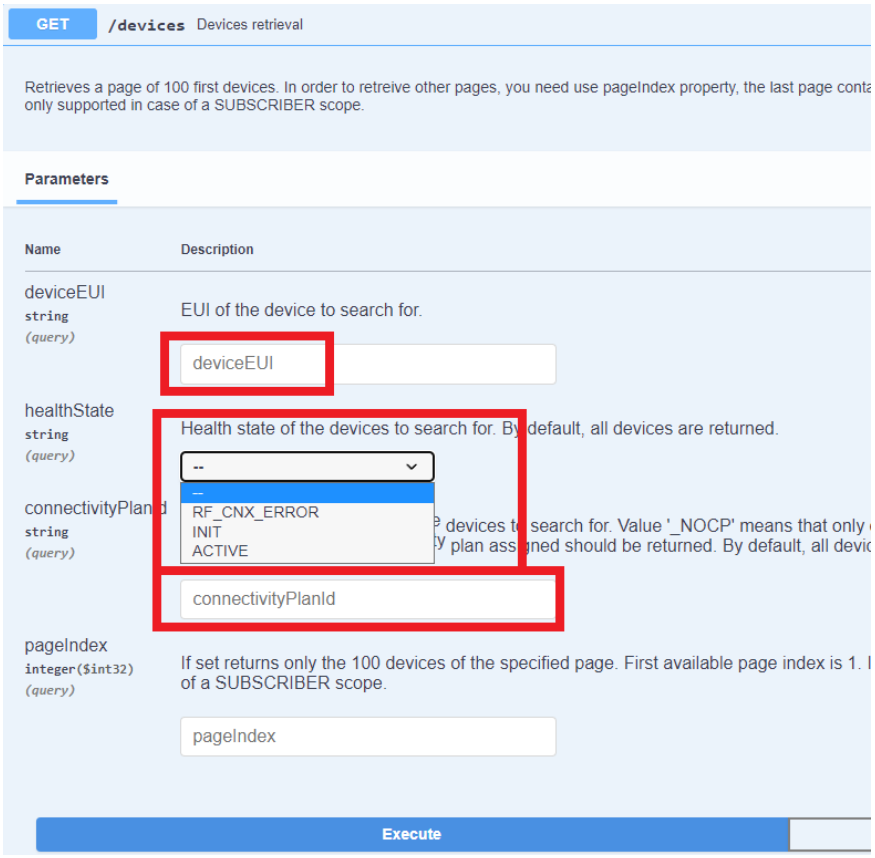

Abbildung 38: Dx-Core API GET Endgeräte

Wir könnten die Suche an dieser Stelle weiter eingrenzen, wählen jedoch im Anwendungsfall keine Einschränkung (die Felder bleiben leer) aus. Danach klicken wir abermals auf „**Execute**“. Da keine Einschränkung vorgenommen wurde, erhält man binnen kürzester Zeit eine Rückmeldung über alle angelegten LPWAN Endkundengeräte und den dazugehörigen Informationen. Zudem ist in der Antwort abermals der im Web-Interface ausgeführte CURL-Befehl für die Command-line Schnittstelle enthalten, um den Befehl von der Ferne auszuführen.

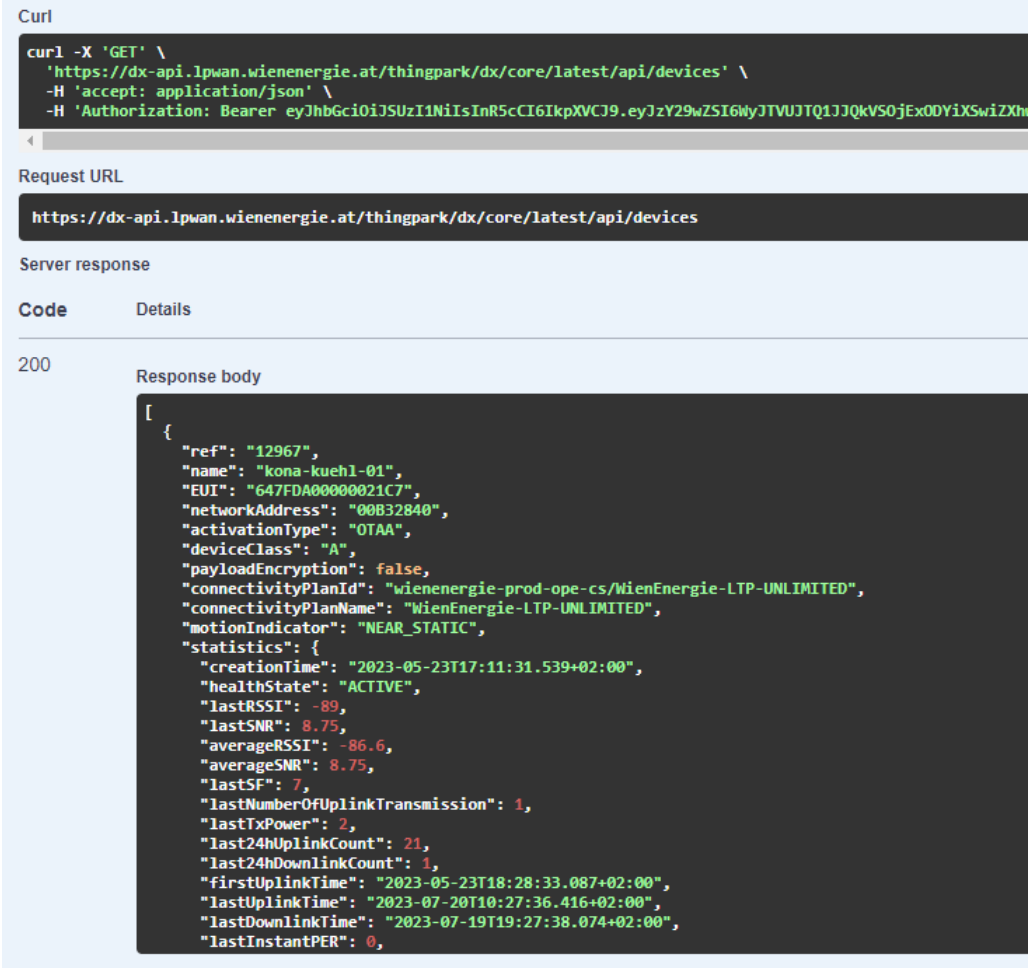

Abbildung 39: DX-Core API Endgeräte Rückmeldung

2.5.4 Senden von Downlink-Nachrichten über die API-Schnittstelle

Neben der Möglichkeit Downlink-Nachrichten aus dem Device Manager (**siehe 2.2.3**) oder über eine ThingPark X Connection - zB. MQTT (**siehe 2.3.3**) - zu senden, gibt es auch den Weg, Downlinks mit Hilfe der API-Schnittstelle in die Warteschlange des LPWAN Netzwerkserver einzureihen. Im Gegensatz zur graphischen Version mit dem Device Manager, erhält man von der API-Schnittstelle sofort eine Rückmeldung, dass die Downlink-Nachricht in die Warteschlange aufgenommen wurde. Außerdem bietet die Schnittstelle (analog zur TPX Connection) mehr Möglichkeiten für die Ausgestaltung der Downlink-Nachricht an.

In der Dx-Core API scrollt man hierfür bis zum Punkt „**Message**“ und klickt auf das Feld „**POST**“. Als Downlink-Nachricht stellen wir die Downlink-Nachricht wie in **Tabelle 3** angeführt, nach.

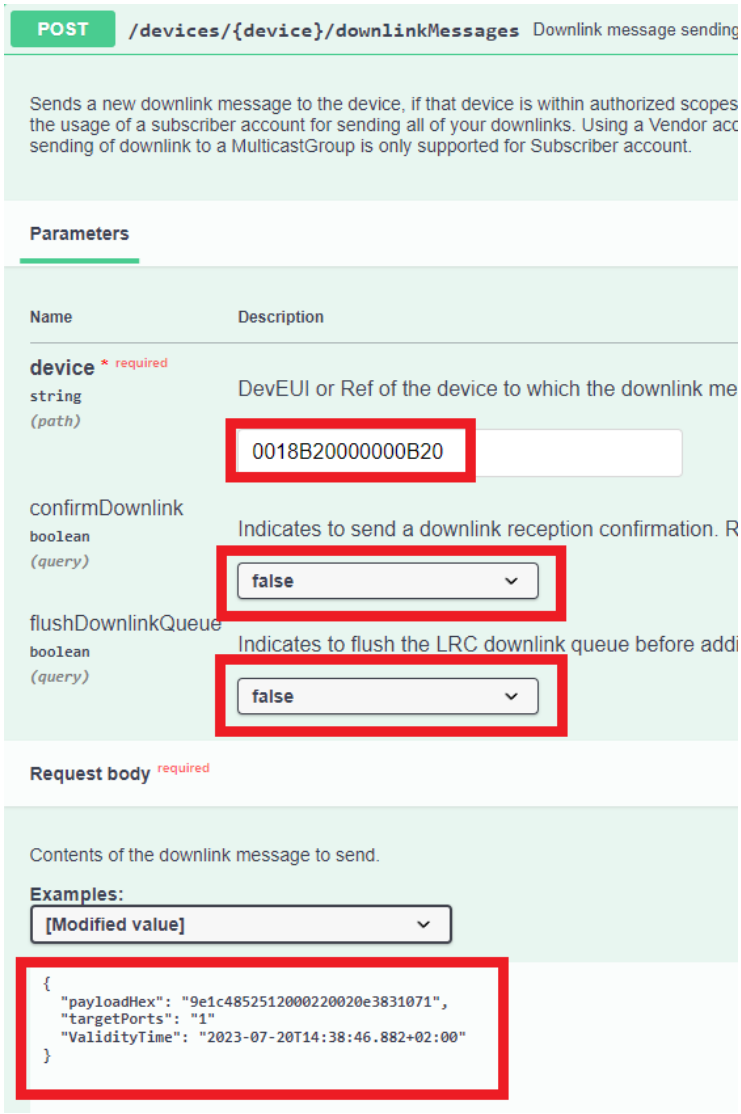

Abbildung 40: Dx-Core API Downlink-Nachricht

Im Unterschied zum Device Manager Downlink (**siehe 2.2.3**) gibt die API-Schnittstelle notwendige Felder außerhalb des Nachrichtenfeld vor. Neben der „**DevEUI**“ besteht die Möglichkeit, dass man die Downlink-Nachricht vom Endkundengerät bestätigt haben möchte („**confirmDownlink**“) und ob die Downlink-Warteschlange gelöscht werden soll („**flushDownlinkQueue**“). Im Nachrichtenfeld befindet sich danach die gewünschte Downlink-Nachricht („**payloadHex**“), das Zielport („**FPort“**) sowie eine Gültigkeitsdauer („**ValidityTime“**), bis wann die Downlink-Nachricht in der Warteschlange stehen soll.

Abermals wird von der API-Schnittstelle ein dazugehöriger **CURL-Befehl** angezeigt, sowie eine Rückmeldung zu der von uns in die Warteschlange aufgenommenen **Downlink-Nachricht**, zurückgemeldet.

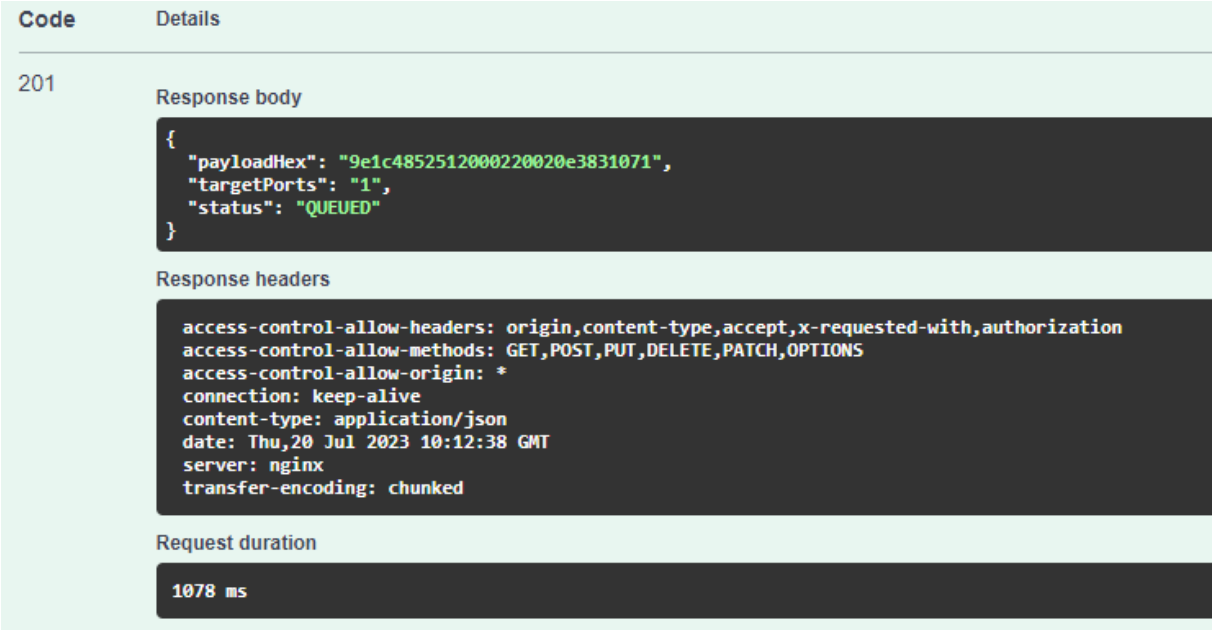

Abbildung 41: Dx-Core API Downlink-Nachricht Rückmeldung

Mit Hilfe dieser Funktionen und den dazugehörigen Rückmeldungen lassen sich unterschiedlichste Prozesse bzw. Logiken aus der Ferne einrichten und prüfen.

Anhang

Abbildungsverzeichnis

Tabellenverzeichnis

Downlink-Nachricht Parameter

Field	Description
Time	ISO 8601 time of the request. Time is mandatory when the Application server authentication has been activated in the AS Profile. In this case the LRC will verify the time deviation between the generation and the reception of the request. The deviation must be lower than Max Time Deviation defined in the AS Profile. Syntax: STRING (ISO date/time).
DevEUI*	Target device IEEE EUI64 in hexadecimal format (representing 8 octets). Syntax: STRING (Hexadecimal representation).
FPort*	Target port (in decimal format). Syntax: NUMBER (Unsigned integer: 1..224).
payload_hex*	Hexadecimal payload. The hexadecimal payload will be encrypted by the LRC cluster if the FCntDn parameter is absent, and if the LRC has been configured with an AppSKey for the specified LoRaWAN® port. Otherwise the payload must be encrypted by the Application Server according to the LoRaWAN® specification, and the FCntDn parameter must be present. The Application Server encryption uses the downlink counter, which is why the FCntDn query parameter is required in this case. Syntax: STRING (Hexadecimal representation).
payload	Decoded payload_hex. Syntax: STRING.
FCntDn	The LoRaWAN® Downlink Counter value is used to encrypt the payload. This query parameter is needed only if the Application server (not the LRC) encrypts the payload. If present, FCntDn will be copied in the LoRaWAN® header field FCnt, and the encrypted payload will be copied as-is to the LoRaWAN® downlink frame by the LRC. Only applicable to LoRaWAN® 1.0. Syntax: NUMBER (32 bits unsigned integer).
AFCntDn	The LoRaWAN® Applicative Downlink Counter value is used to encrypt the payload. This query parameter is needed only if the Application server (not the LRC) encrypts the payload. If present, AFCntDn will be copied in the LoRaWAN® header field FCnt, and the encrypted payload will be copied as-is to the LoRaWAN® downlink frame by the LRC. Only applicable to LoRaWAN® 1.1. Syntax: NUMBER (32 bits unsigned integer).
Confirmed	A value of Confirmed=0 requests transmission of an UNCONFIRMED downlink frame. A value of Confirmed=1 requests transmission of a CONFIRMED downlink frame. Default value is Confirmed=0 (UNCONFIRMED). Support of Confirmed frame transmission is subject to Connectivity plan feature flag ackedDownlinkFrame. If the Confirmed flag is set on the HTTP POST and the device is associated with a Connectivity plan where the ackedDownlinkFrame feature flag is set, the downlink packet is processed. Otherwise the processing is aborted, and a specific error code is returned to the AS in the HTTP response. When targeting a multicast device, only unconfirmed frame is supported. Syntax: NUMBER (Unsigned integer: 0..1).
FlushDownlinkQueue	Empties the device AS downlink queue of the device (Boolean). When this parameter is set to FlushDownlinkQueue=1, the AS requests the LRC to purge the AS downlink queue of the device prior to add the downlink payload transported by this HTTP POST. Syntax: NUMBER (Unsigned integer: 0..1).

Field	Description
ValidityTime	Associates the AS downlink payload with an expiration date (ISO 8601 timestamp or Duration in seconds) in the device AS downlink queue. If the AS downlink payload has not yet been sent to the device, the AS downlink payload will be discarded by the LRC when the expiration date is reached. Syntax: STRING (ISO date/time) or NUMBER (Unsigned integer).
AS_ID	Application Server ID, as provisioned in the AS Profile. AS_ID is mandatory if the Application server authentication has been activated in the AS Profile. In this case, the LRC will check that the Application Server is authorized to send downlink command to the device. Syntax: STRING.
AS_KEY	Application Server Key. Syntax: STRING.
Token	Security token to sign the downlink frame. Token is mandatory when the Application server authentication has been activated in the AS Profile. Syntax: STRING (256 bits hexadecimal).
CorrelationID	64 bits ID used to correlate the downlink frame with the associated downlink frame sent report or multicast summary reports. When this parameter is provided, it is sent back in the associated downlink frame sent report for unicast downlink frame or in the associated multicast summary reports for multicast downlink frame. Syntax: STRING (64 bits hexadecimal).
RetryIneligibleGateways	When set to 1 or not provided, non eligible gateways (GPS out of sync for Class B, gateway down for Class B/C…) are retried during each retransmission attempt. When set to 0, non eligible gateways are excluded at the beginning of the multicast campaign and not retried during each retransmission attempt. This parameter is only applicable to multicast downlink transmission. Syntax: NUMBER (Unsigned integer: 0..1).