Making IOT great again

Our journey to save EV chargers from trash

[TLP:GREEN]

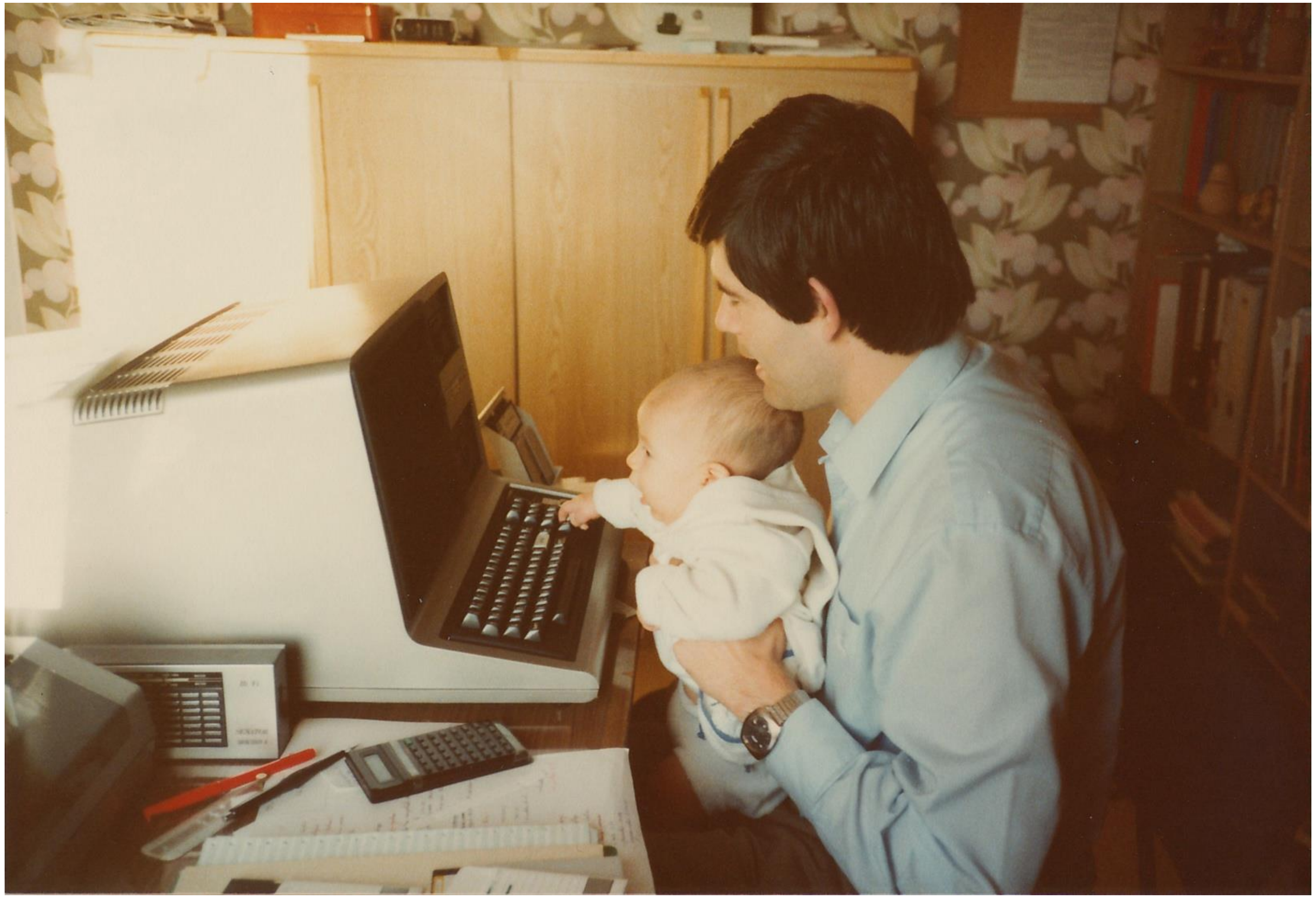
Disclaimer

- This presentation **does not** reflect the opinion of our employer.
- There is no judgment against the company behind the product.
- All the efforts were made to save appliances from being useless, nothing more.

[TLP:GREEN]

Who are we?

- **David Durvaux**
  - Engineer in computer sciences
  - Working in cybersecurity during the day
  - Enjoy to understand how things works…for a long time
- **Marc Durvaux**
  - PhD in electronics and telecommunication
  - Spent his career the R&D for telecommunication and space systems
  - Enjoy building electronic devices and low-level programming



[TLP:GREEN]

Agenda

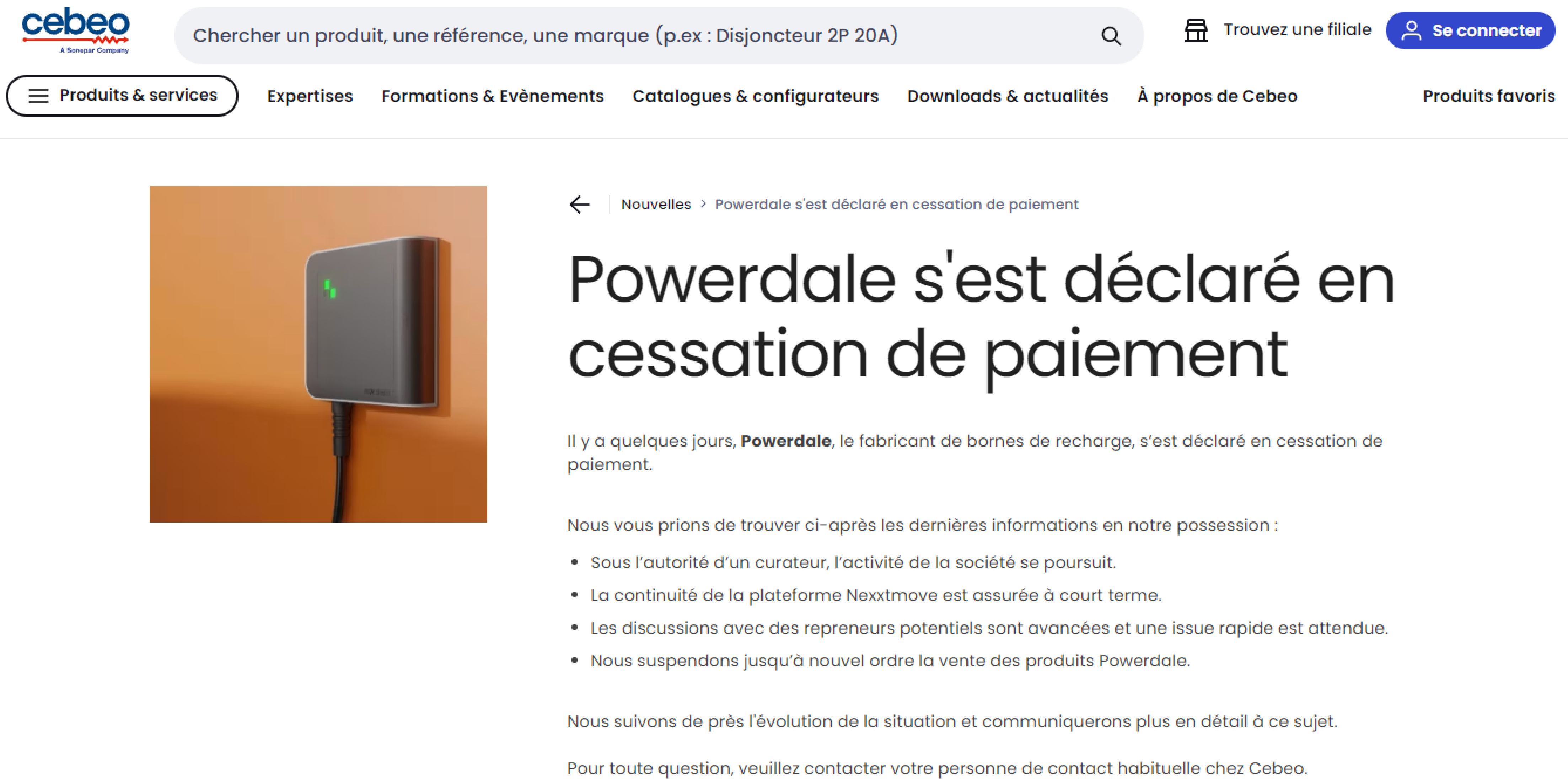
1 The story of Powerdale Nexxtender Home

2 Our journey toward a solution

3 Reflection on IOT todays

4 Conclusion

What happened?


cebeo
A Sonepar Company
Chercher un produit, une référence, une marque (p.ex : Disjoncteur 2P 20A)
Trouvez une filiale
Se connecter
Produits & services
Expertises
Formations & Evènements
Catalogues & configurateurs
Downloads & actualités
À propos de Cebeo
Produits favoris
Nouvelles > Powerdale s'est déclaré en cessation de paiement

Powerdale s'est déclaré en cessation de paiement

Il y a quelques jours, **Powerdale**, le fabricant de bornes de recharge, s'est déclaré en cessation de paiement.

Nous vous prions de trouver ci-après les dernières informations en notre possession :

- Sous l'autorité d'un curateur, l'activité de la société se poursuit.
- La continuité de la plateforme Nexxtmove est assurée à court terme.
- Les discussions avec des repreneurs potentiels sont avancées et une issue rapide est attendue.
- Nous suspendons jusqu'à nouvel ordre la vente des produits Powerdale.

Nous suivons de près l'évolution de la situation et communiquerons plus en détail à ce sujet.

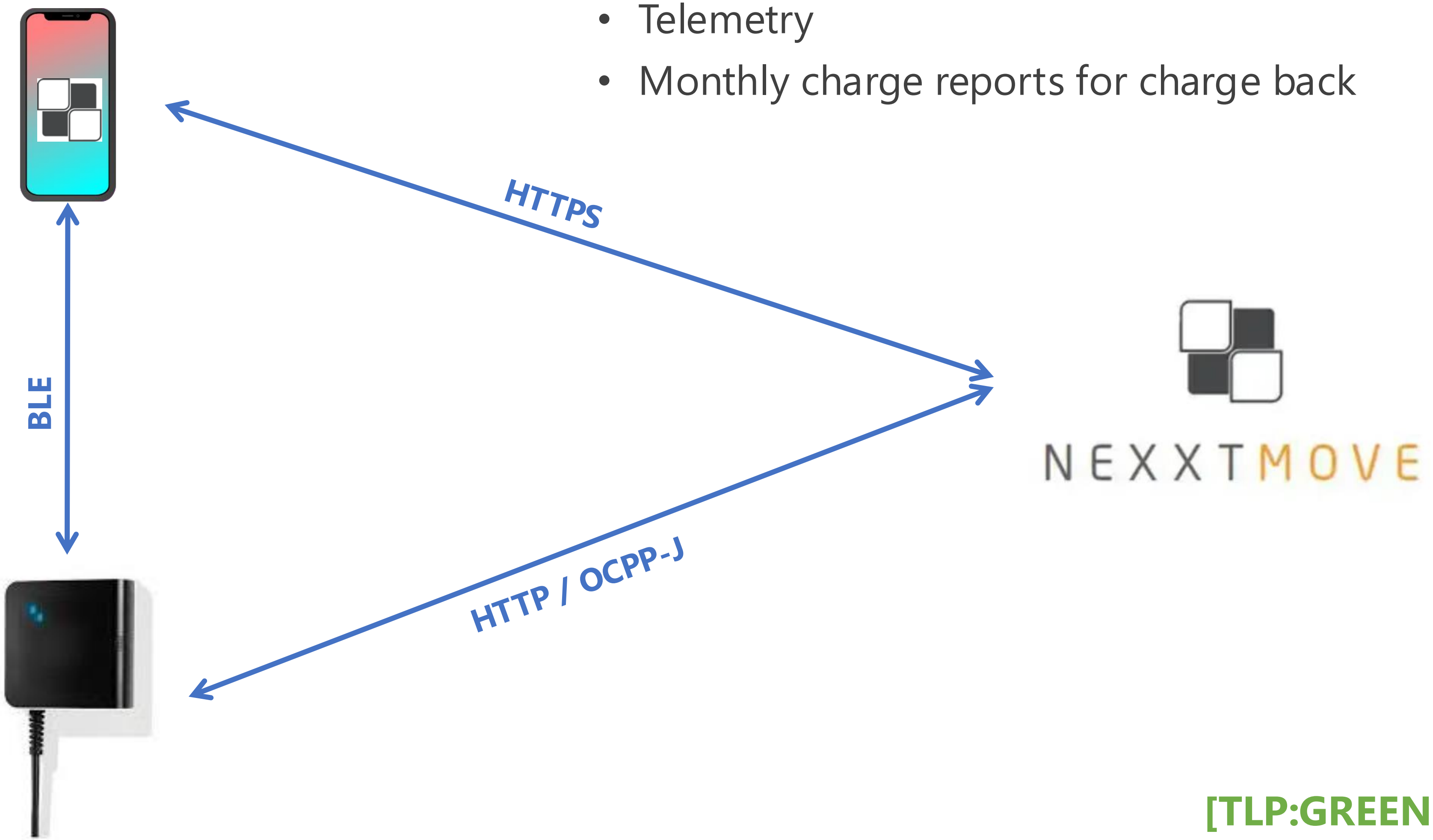
Pour toute question, veuillez contacter votre personne de contact habituelle chez Cebeo.

[TLP:GREEN]

Powerdale ecosystem in a nutshell

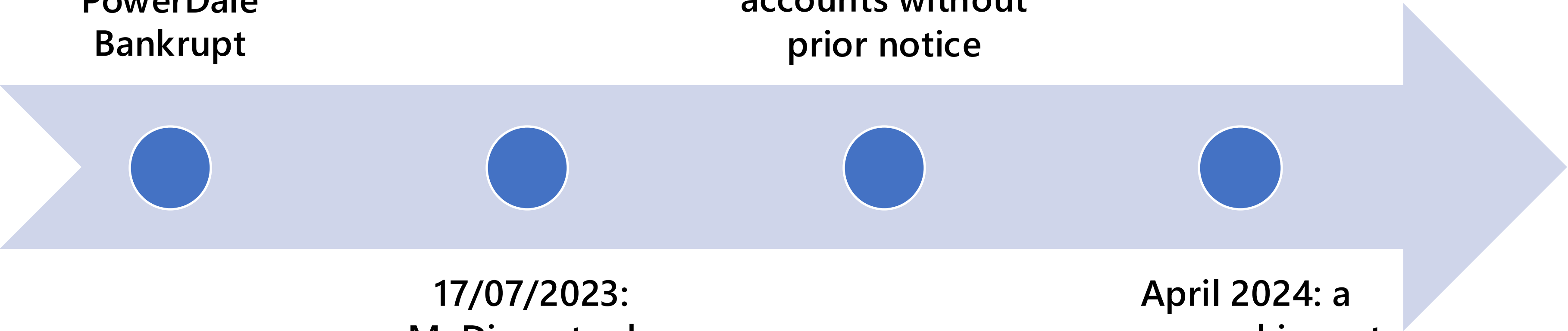
- Nexxtmove mobile app
  - Configure the charger
  - Collect data if WiFi is disabled
  - Upload data to nexxtmove cloud platoform

- Nexxtmove.me
  - Authentication
  - Telemetry
  - Monthly charge reports for charge back



[TLP:GREEN]

Impact timeline

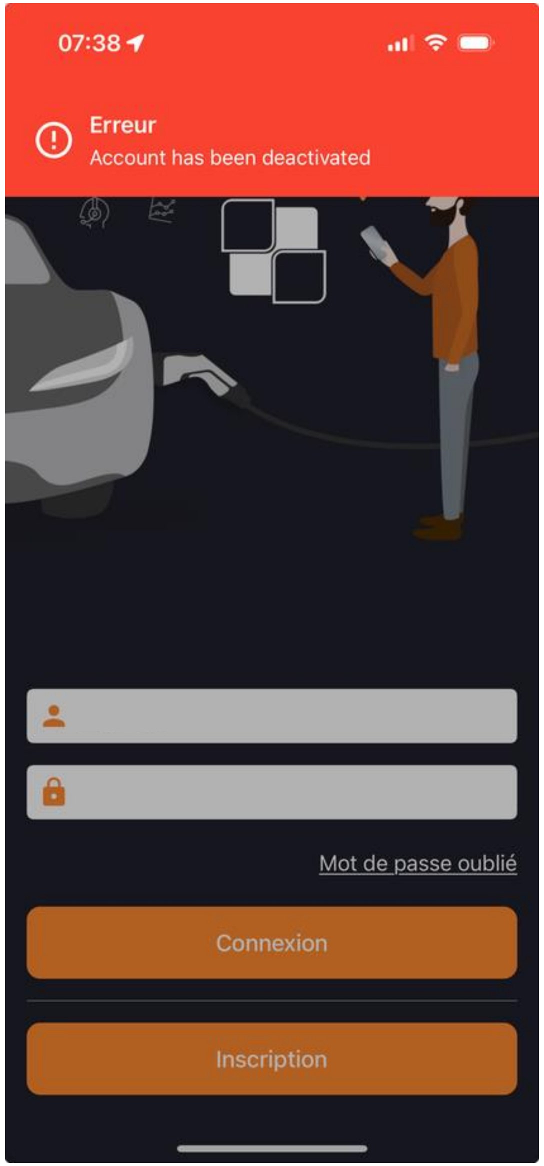


26/06/2023: PowerDale Bankrupt

17/07/2023: MyDiego took over Neextmove

February 2024: MyDiego removed customers accounts without prior notice

April 2024: a command is sent over Internet to downgrade chargers to 6A max



07:38

Erreur

Account has been deactivated

Real impact for resellers, installers and customers?

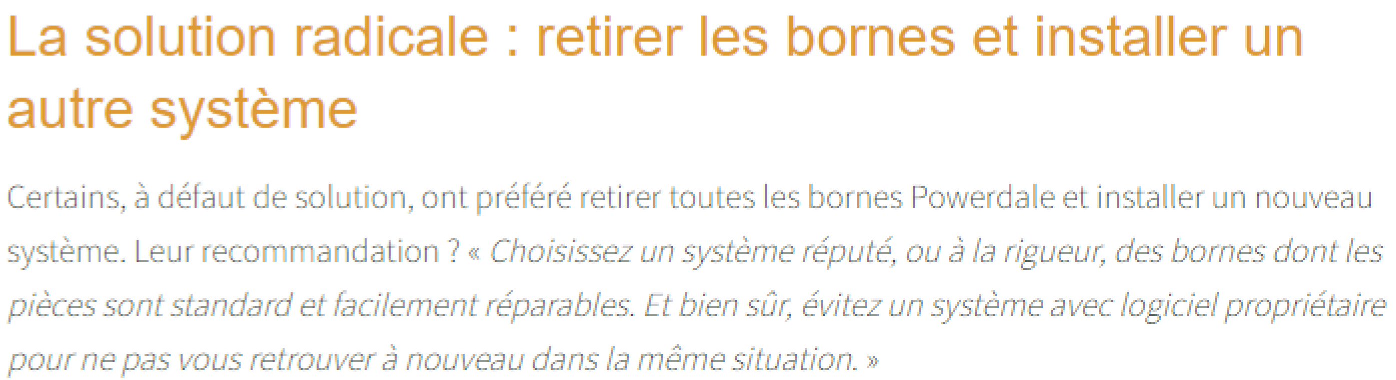
- Hardware becomes unmaintained
- About 50.000 appliances installed in the Benelux
- Heavy stock (around 2000) of appliances for some resellers
- Some installers get prosecuted by their customers for
  - Not being able to charge anymore
  - Degraded service to 6A, the minimal current to allow charging (instead of up to 3x 32A)
  - ...
- Customers are unable to charge except if
  - they accept a 6A limit (or have a version without WiFi enabled)
  - They had configured beforehand the charger in "Open" mode
    - Anyone can charge without any restriction...

Now we have a challenge but no working communication with the EV charger...

Picture generated by Microsoft Copilot

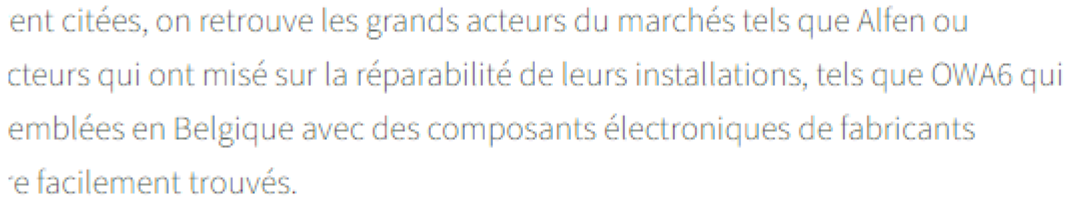
[TLP:GREEN]

The "official" advice? Let's trash it...



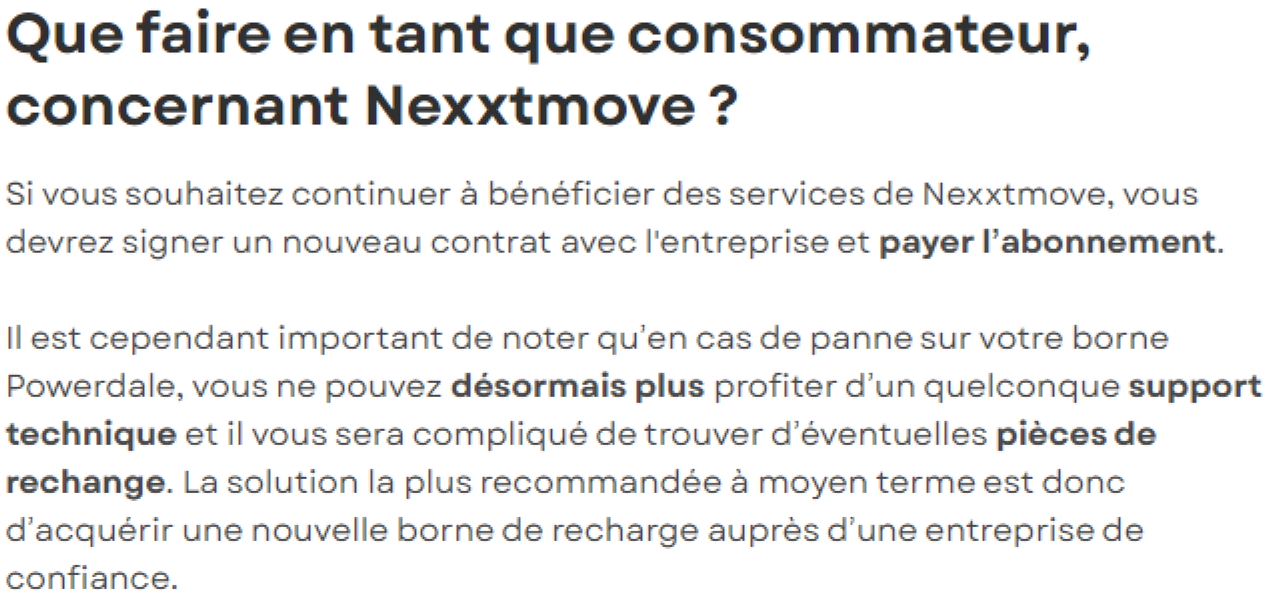
La solution radicale : retirer les bornes et installer un autre système

Certains, à défaut de solution, ont préféré retirer toutes les bornes Powerdale et installer un nouveau système. Leur recommandation ? « *Choisissez un système réputé, ou à la rigueur, des bornes dont les pièces sont standard et facilement réparables. Et bien sûr, évitez un système avec logiciel propriétaire pour ne pas vous retrouver à nouveau dans la même situation.* »



ent citées, on retrouve les grands acteurs du marchés tels que Alfen ou
cteurs qui ont misé sur la réparabilité de leurs installations, tels que OWA6 qui
emblées en Belgique avec des composants électroniques de fabricants
'e facilement trouvés.

Union Wallonne des Entreprise
on 26/04/2024



Que faire en tant que consommateur, concernant Nexxtmove ?

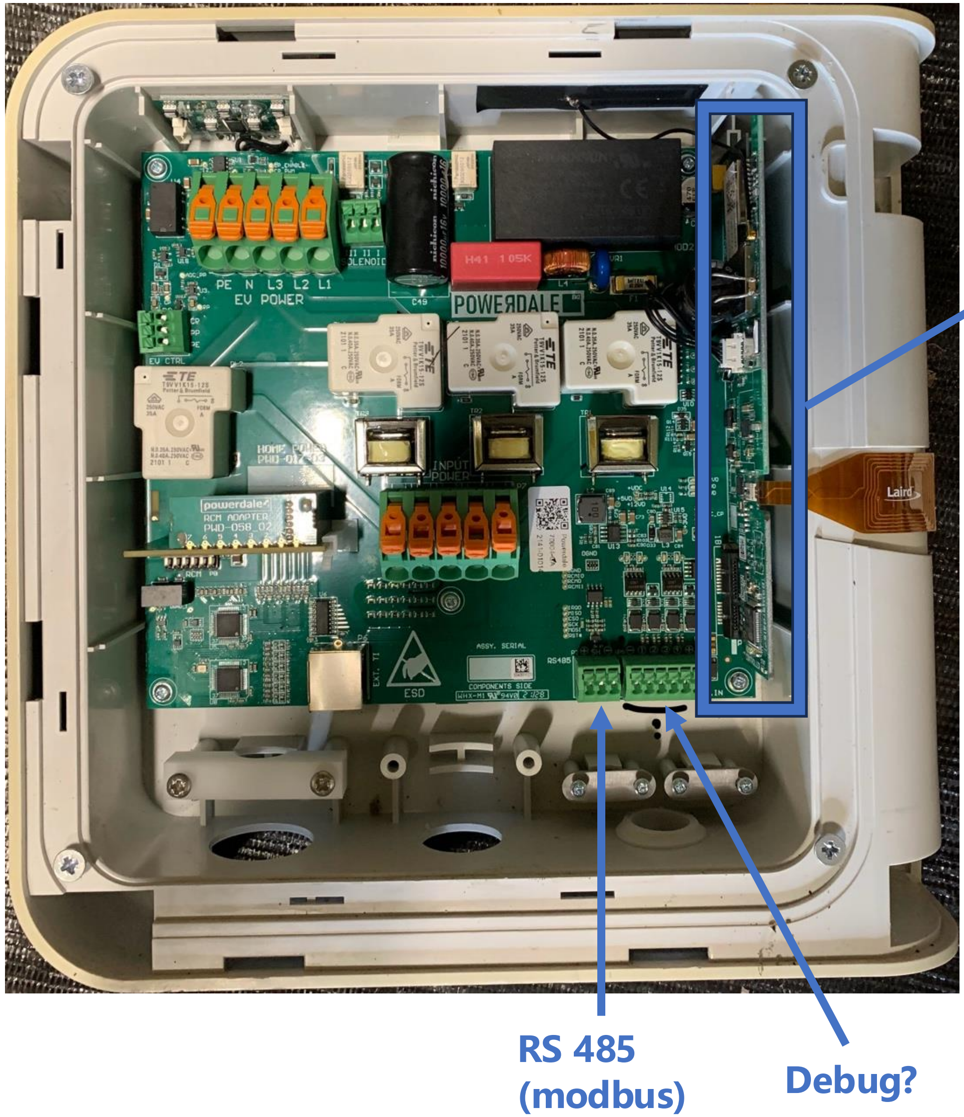
Si vous souhaitez continuer à bénéficier des services de Nexxtmove, vous devrez signer un nouveau contrat avec l'entreprise et **payer l'abonnement**.

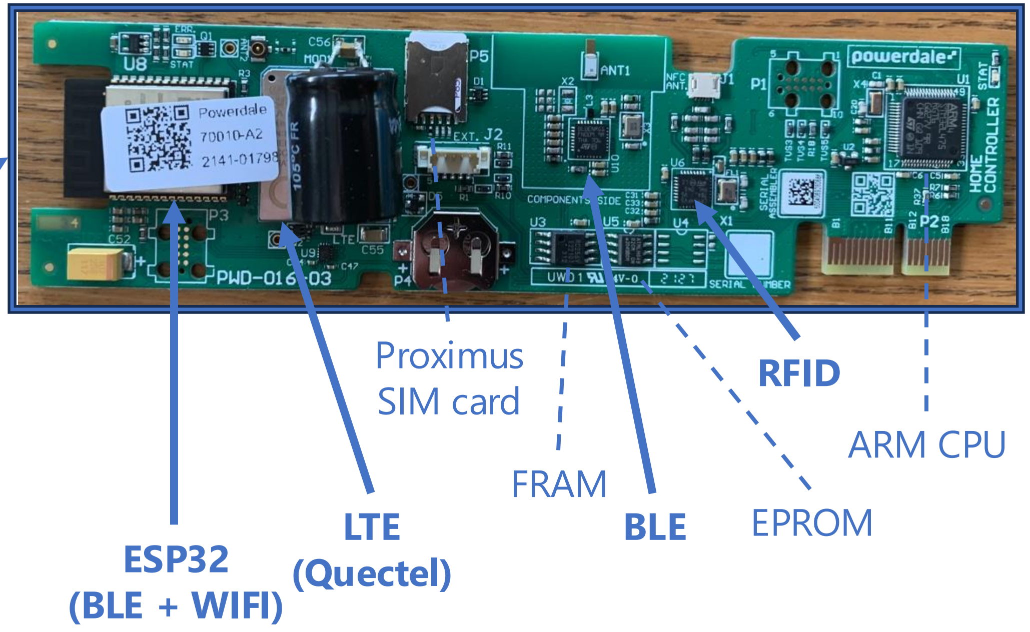
Il est cependant important de noter qu'en cas de panne sur votre borne Powerdale, vous ne pouvez **désormais plus** profiter d'un quelconque **support technique** et il vous sera compliqué de trouver d'éventuelles **pièces de rechange**. La solution la plus recommandée à moyen terme est donc d'acquérir une nouvelle borne de recharge auprès d'une entreprise de confiance.

Test Achat on 17/05/2024

[TLP:GREEN]

Available communication channels





- Powerdale datasheet mentions for the Nexxtender Home product:
  - WIFI (later)
  - Bluetooth
  - OSCP (Open Smart Charging Protocol)
  - OCCP (Open Charge Point Protocol)
    - Use to communicate with Nexxtmove

How did we gain back access?

- A mix of reversing and a nice **collaborative effort!**
  - User and installer applications were still available in Google Play Store and Apple App Store
  - ESPHome BLE Client for Powerdale Nexxtender EV Charger from Geert Meersman
    - Already include most of the BLE protocol
    - Developed as an integration with Home Assistant
  - nexxtender-ble offering a basic Bluetooth communication implementation via a PicoW

- As usually:
  - You are not alone on the idea ☺
  - You are stronger working with others

- Authentication with the appliance?
  - PIN code generation algorithm is in the installer app
    - Lessons learned: if there are 2 apps, might be good to look at both ;)
    - It is actually a vulnerability: from visible appliances, you can find the PIN and control it ☹

An insight into the BLE protocol

Note : an in-depth description of BLE protocol is well beyond the scope of this talk

- First step: detect the presence of the charging station (the peripheral)
  - The peripheral broadcasts advertising messages
  - The central device initiates an active scanning

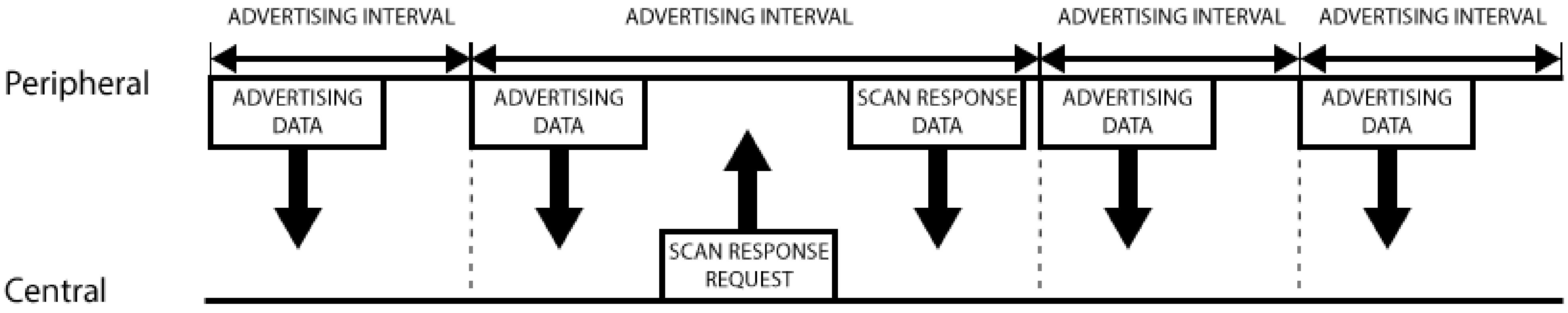


Figure source : https://learn.adafruit.com/introduction-to-bluetooth-low-energy

- From the device(s) responses, collect MAC address and device name
  - The latter let us known that it is a Powerdale charging station ==> stop scanning

[TLP:GREEN]

An insight into the BLE protocol (cont'd)

- Second step: establish a secured communication channel
  - Create client
  - Send "connect to device" command
  - Send "secure connection" command
    - Provide PIN code when receiving call-back "passkey request"
  - Check the connection
    - Get device information in reading characteristics of "device information service"
    - Compare product number and serial number to stored values
      - Avoid to connect to another charging station in the radio coverage area
- Third step: enter communication loop
  - Initialize callbacks from the "receive service"
    - Process data from callbacks asynchronously (e.g. data measurements)
  - Send periodic time sync commands
  - Send configuration and operational commands on request

GATT transactions

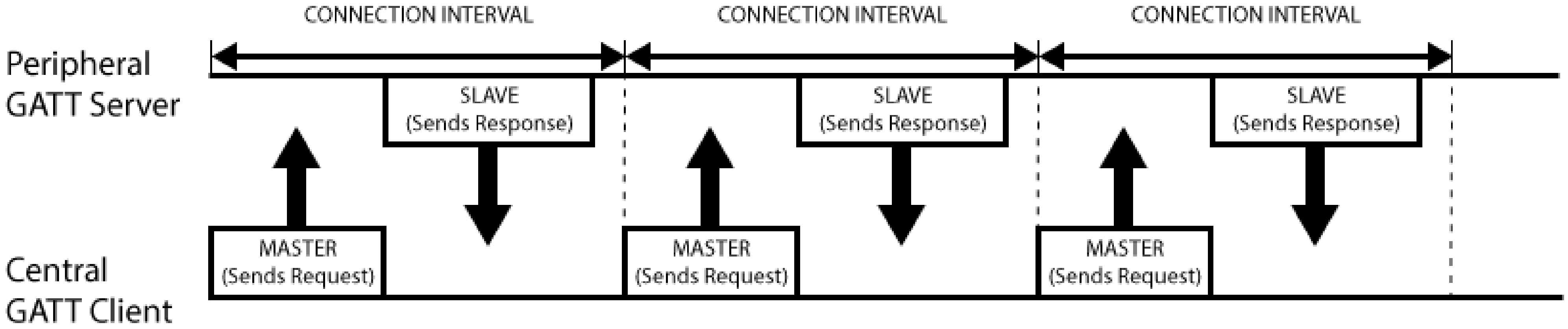


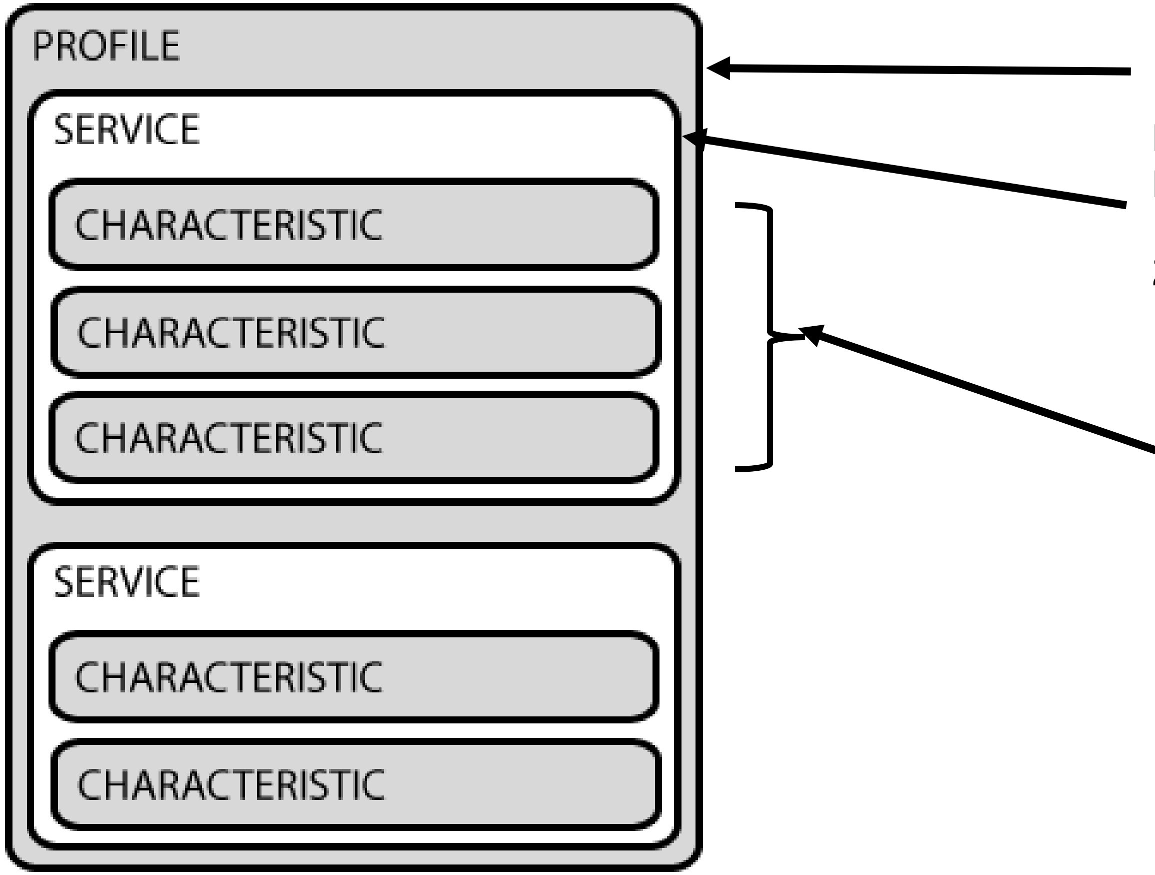
Figure source : https://learn.adafruit.com/introduction-to-bluetooth-low-energy

- GATT server:
  - hold the Attribute Profile (ATT) lookup data
  - Service and characteristic definition
- GATT client: sends requests to the service (incl. writing characteristics)

Source: https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt

[TLP:GREEN]

GATT messages



Defined by the BLE peripheral itself.

Break data in logical entities containing chunk of data. Distinguished by its UUID:

1) 16 bits UUID for official BLE services
2) 128 bits UUID for custom services

Data chunk (1..N per service)

1. Pre-defined 16 bits UUID
2. Custom 128 bits UUID

Encapsulate a single data point (which could be an array)

Source: https://learn.adafruit.com/introduction-to-bluetooth-low-energy

An insight into the BLE protocol (cont'd)

- Commands are sent to the charging station by writing to a single characteristic
  - Configuration parameters
  - Time
    - The charging station has (no) more direct Internet access
    - The ESP32 gateway acts as a NTP client
  - Start / Stop charging Eco or Max in the open and private modes
- Responses are received as notifications
  - Spontaneous (measurements)
  - Results from a command (e.g. read parameters)
    - Data are packed in 128 bits word that have to be parsed

- *ESP32 implementation based on the NimBLE library*

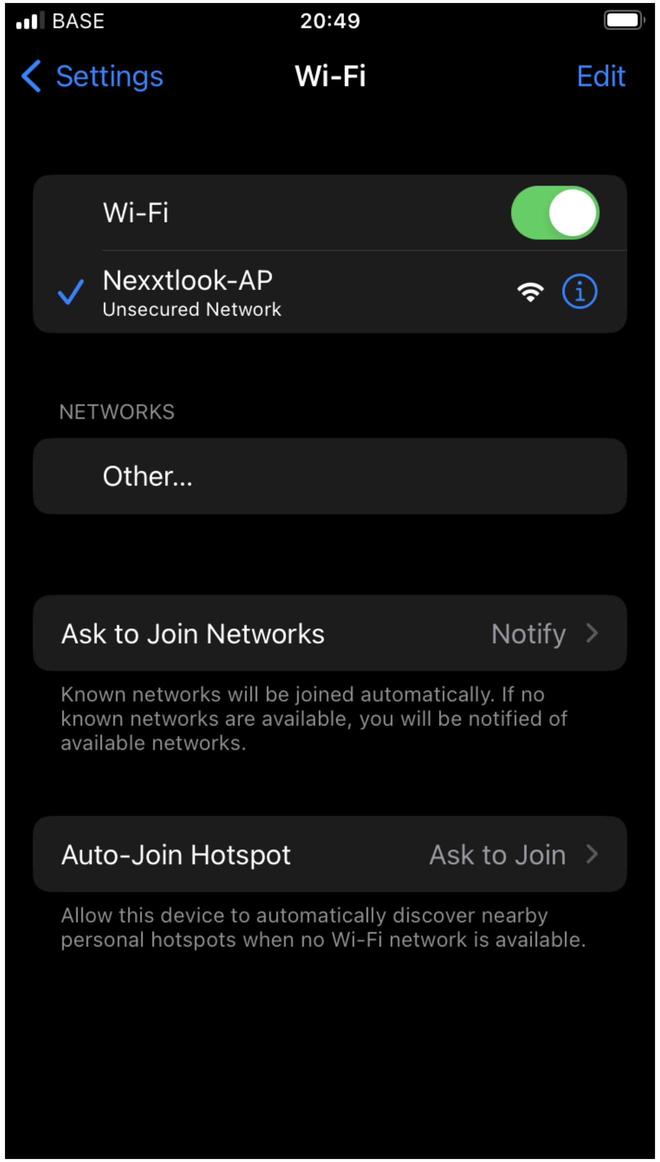
A few words on the software architecture

- *Hardware constraints*
  - *~380 kB RAM*
  - *1 physical radio for both WiFi and BLE*
- *Off-the-shelves libraries*
  - *BLE, WiFi, Webserver, NTP client, MQTT client, SPIFFS*
- *FreeRTOS running in background*
  - *Stack size / process ~8kB*
  - *Watchdogs defined in libraries*
  - *> 6 asynchronous processes*

→ *Static buffers for "large" arrays*

→ *Flags to trigger "long" activities in background loop*
e.g. send BLE command, publish MQTT message, write to file system

Demo – Module setup



BASE 20:49

< Settings Wi-Fi Edit

Wi-Fi ●

✓ Nexxtlook-AP
Unsecured Network

NETWORKS

Other...

Ask to Join Networks Notify >

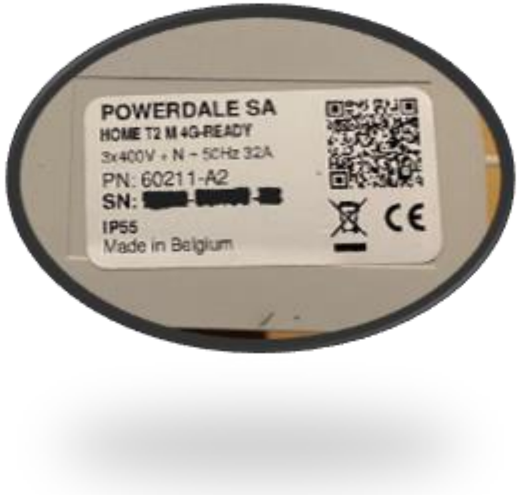
Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.

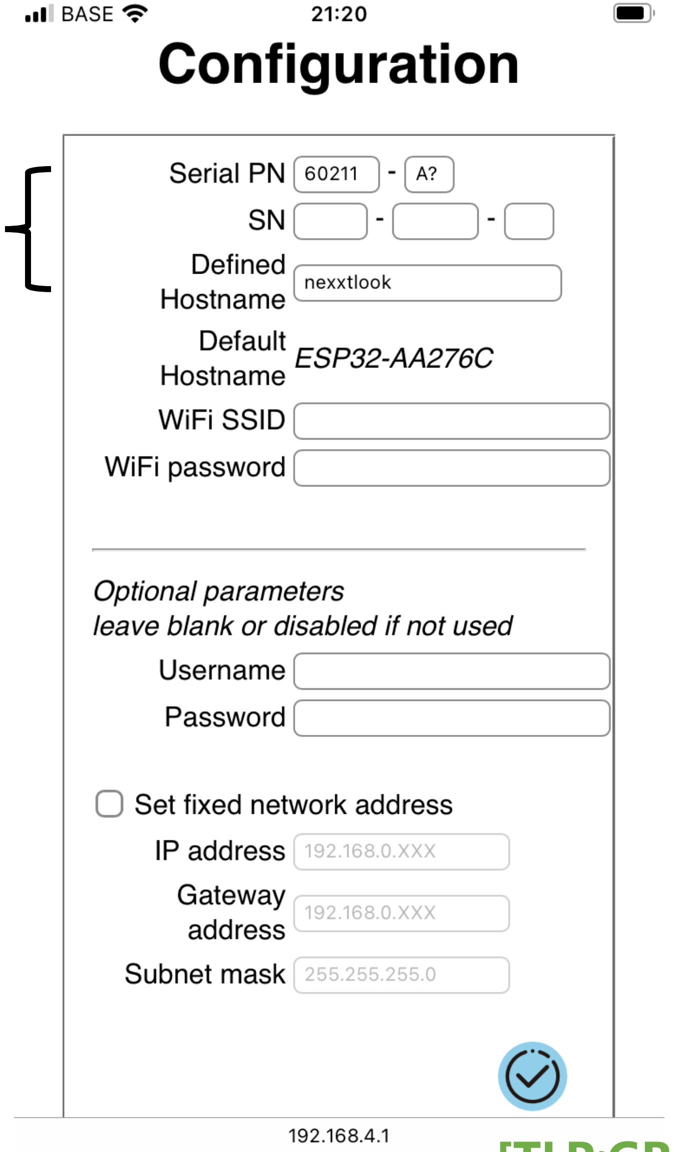
Auto-Join Hotspot Ask to Join >

Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.

ESP32 exposed itself as an access point running a small webserver waiting for initial configuration

All the parameters needed to generate the PIN code ☺





BASE 21:20

Configuration

Serial PN 60211 - A?

SN [ ] - [ ] - [ ]

Defined Hostname nexxtlook

Default Hostname *ESP32-AA276C*

WiFi SSID

WiFi password

Optional parameters
leave blank or disabled if not used

Username

Password

□ Set fixed network address

IP address 192.168.0.XXX

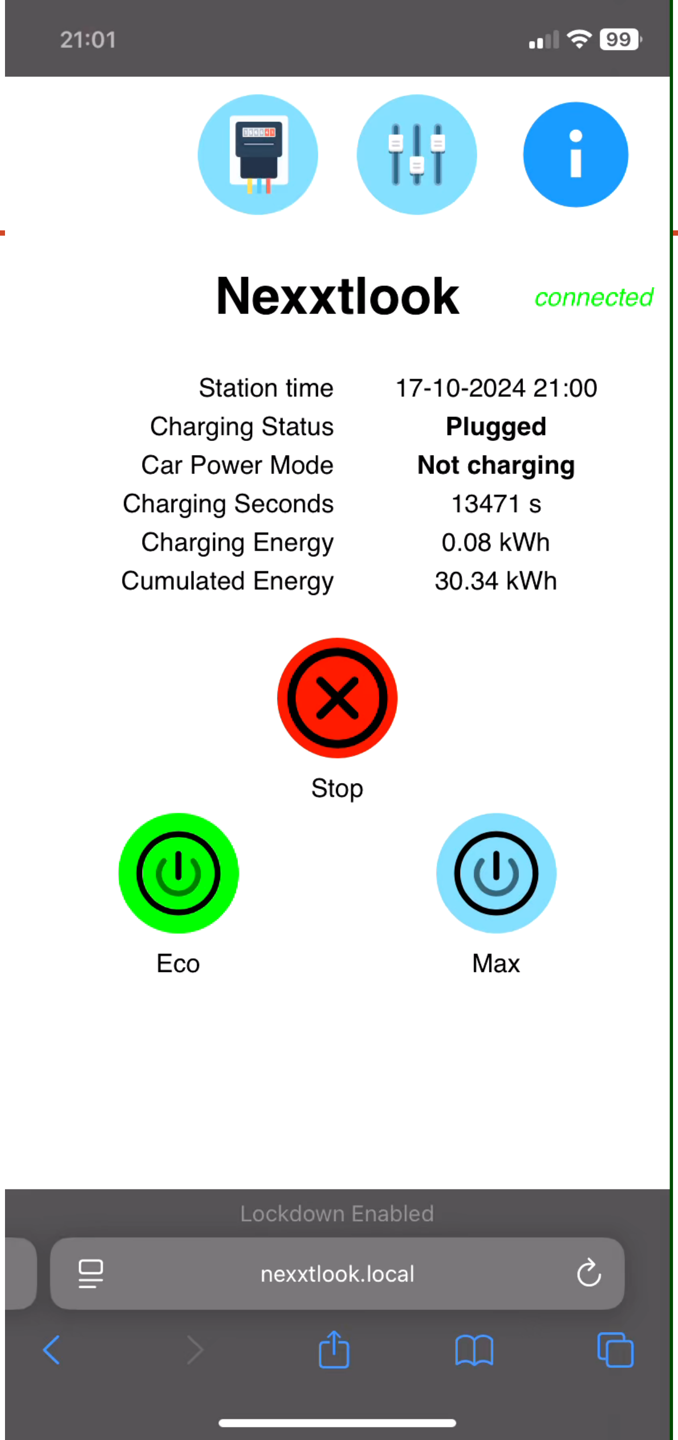
Gateway address 192.168.0.XXX

Subnet mask 255.255.255.0

192.168.4.1

[TLP:GREEN]

Demo – Appliance Operation

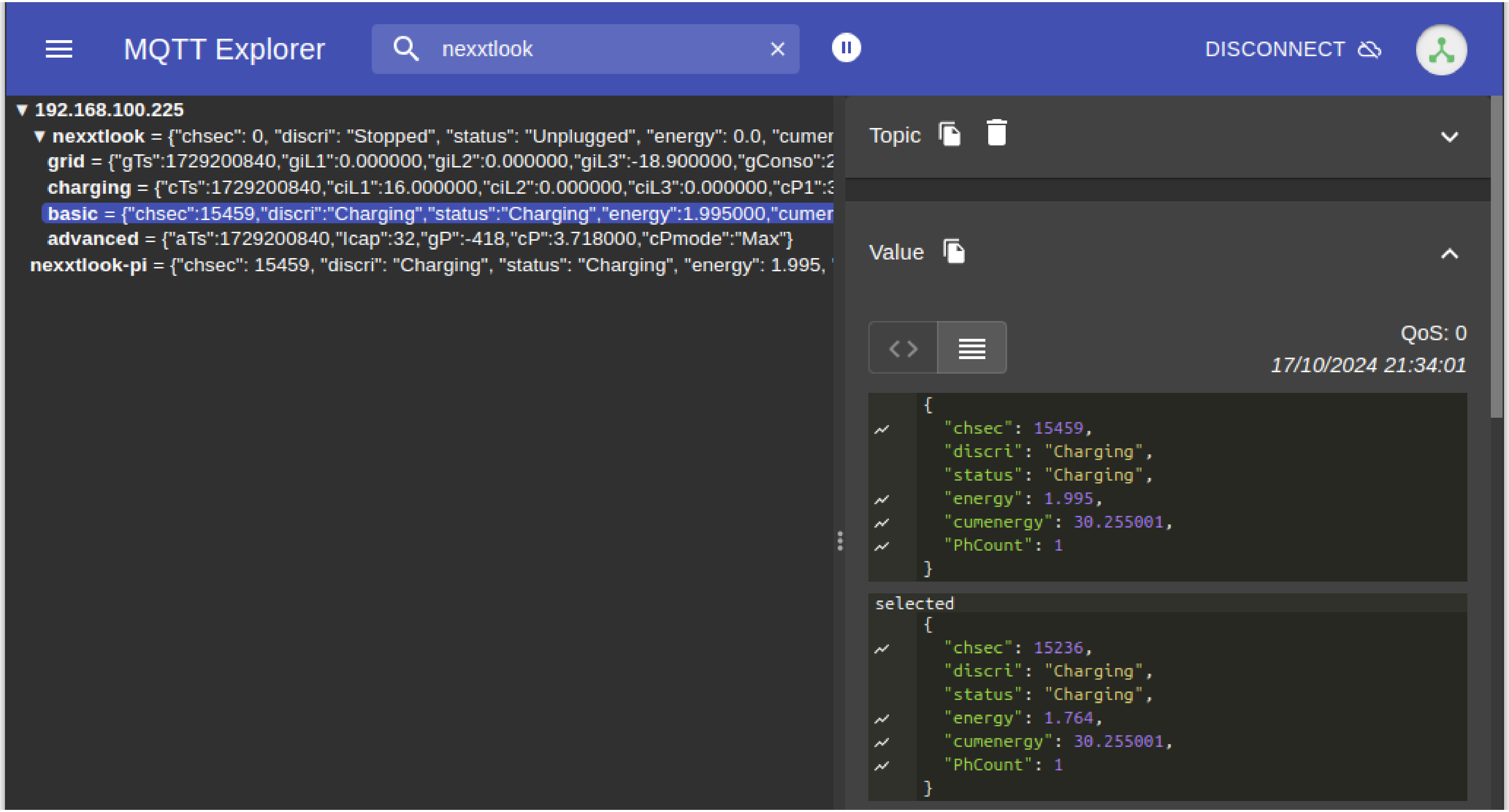


Nexxtlook *connected*

Station time	17-10-2024 21:00
Charging Status	**Plugged**
Car Power Mode	**Not charging**
Charging Seconds	13471 s
Charging Energy	0.08 kWh
Cumulated Energy	30.34 kWh

[TLP:GREEN]

Demo – MQTT data



```
▼ 192.168.100.225
  ▼ nexxtlook = {"chsec": 0, "discri": "Stopped", "status": "Unplugged", "energy": 0.0, "cumer
      grid = {"gTs":1729200840,"giL1":0.000000,"giL2":0.000000,"giL3":-18.900000,"gConso":2
      charging = {"cTs":1729200840,"ciL1":16.000000,"ciL2":0.000000,"ciL3":0.000000,"cP1":3
      basic = {"chsec":15459,"discri":"Charging","status":"Charging","energy":1.995000,"cumer
      advanced = {"aTs":1729200840,"Icap":32,"gP":-418,"cP":3.718000,"cPmode":"Max"}
    nexxtlook-pi = {"chsec": 15459, "discri": "Charging", "status": "Charging", "energy": 1.995, '
```

QoS: 0

17/10/2024 21:34:01

```
{
  "chsec": 15459,
  "discri": "Charging",
  "status": "Charging",
  "energy": 1.995,
  "cumenergy": 30.255001,
  "PhCount": 1
}
```

```
selected
{
  "chsec": 15236,
  "discri": "Charging",
  "status": "Charging",
  "energy": 1.764,
  "cumenergy": 30.255001,
  "PhCount": 1
}
```

[TLP:GREEN]

Powerdale Neextender Home owner?

Picture generated by Microsoft Copilot

- There are now at least 4 solutions:
  1. Pay a subscription to nexxtmove.me
  2. Use one of the 3 projects which implement the protocol to connect with your appliance
     - All offers the minimal sets of features to enable again the appliance and charge a car.

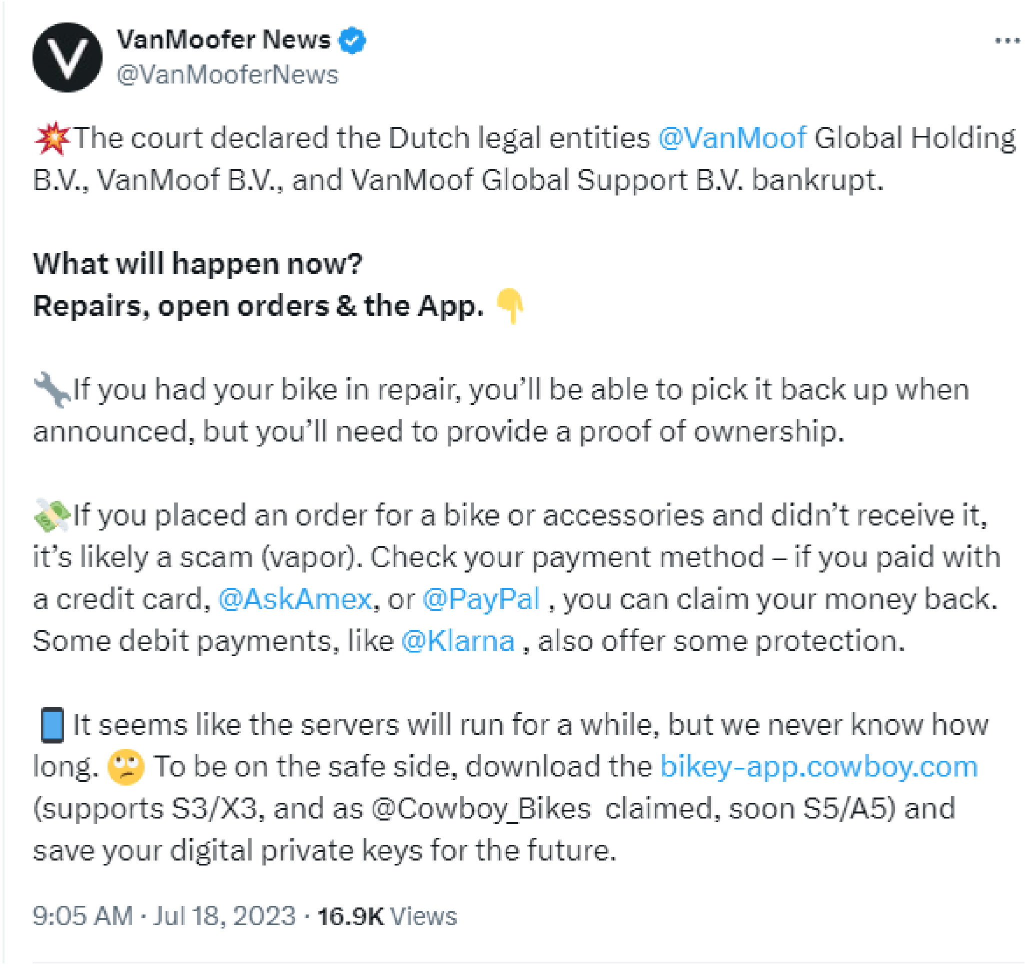
[TLP:GREEN]

To be or not to be open-source?

- We are big supporter of open-source but...
  - How to prevent abuse and illegal uses?
    - Some safeguard in the code
      - Can be associated only once to an EV charger
    - The PIN code vulnerability cannot be fixed
  - Distribute the solution as a "full" package through a Powerdale appliance reseller
- Published implementation are only partial to address this issue

Picture generated by Microsoft Copilot

“What happened with Powerdale is an exception...”



VanMoofer News @VanMooferNews

💥The court declared the Dutch legal entities @VanMoof Global Holding B.V., VanMoof B.V., and VanMoof Global Support B.V. bankrupt.

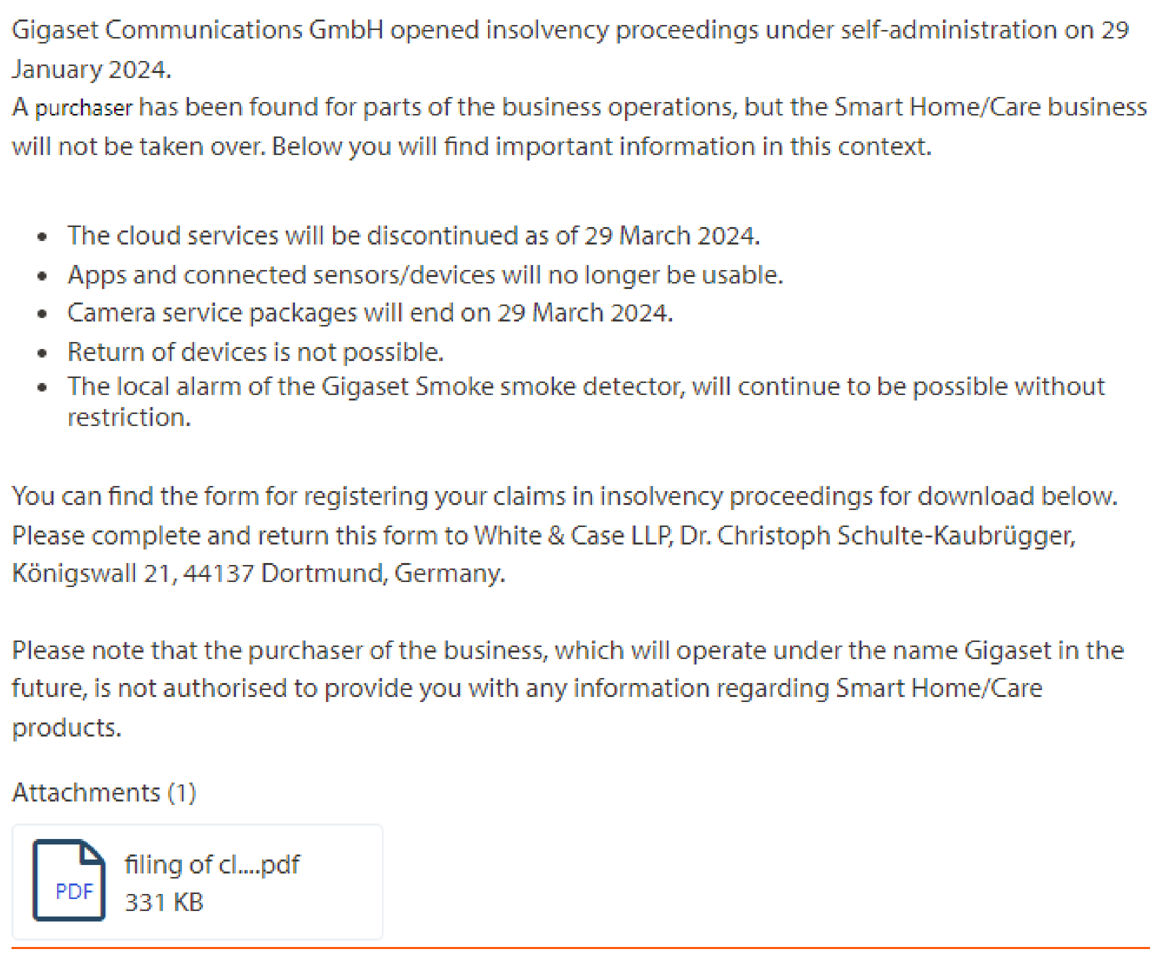
What will happen now?
Repairs, open orders & the App. 👇

🔧If you had your bike in repair, you’ll be able to pick it back up when announced, but you’ll need to provide a proof of ownership.

💸If you placed an order for a bike or accessories and didn’t receive it, it’s likely a scam (vapor). Check your payment method – if you paid with a credit card, @AskAmex, or @PayPal , you can claim your money back. Some debit payments, like @Klarna , also offer some protection.

📱It seems like the servers will run for a while, but we never know how long. 🙄 To be on the safe side, download the bikey-app.cowboy.com (supports S3/X3, and as @Cowboy_Bikes claimed, soon S5/A5) and save your digital private keys for the future.

9:05 AM · Jul 18, 2023 · **16.9K** Views



Gigaset Communications GmbH opened insolvency proceedings under self-administration on 29 January 2024.
A purchaser has been found for parts of the business operations, but the Smart Home/Care business will not be taken over. Below you will find important information in this context.

- The cloud services will be discontinued as of 29 March 2024.
- Apps and connected sensors/devices will no longer be usable.
- Camera service packages will end on 29 March 2024.
- Return of devices is not possible.
- The local alarm of the Gigaset Smoke smoke detector, will continue to be possible without restriction.

You can find the form for registering your claims in insolvency proceedings for download below. Please complete and return this form to White & Case LLP, Dr. Christoph Schulte-Kaubrügger, Königswall 21, 44137 Dortmund, Germany.

Please note that the purchaser of the business, which will operate under the name Gigaset in the future, is not authorised to provide you with any information regarding Smart Home/Care products.

Attachments (1)

PDF filing of cl....pdf
331 KB

And many others...

[TLP:GREEN]

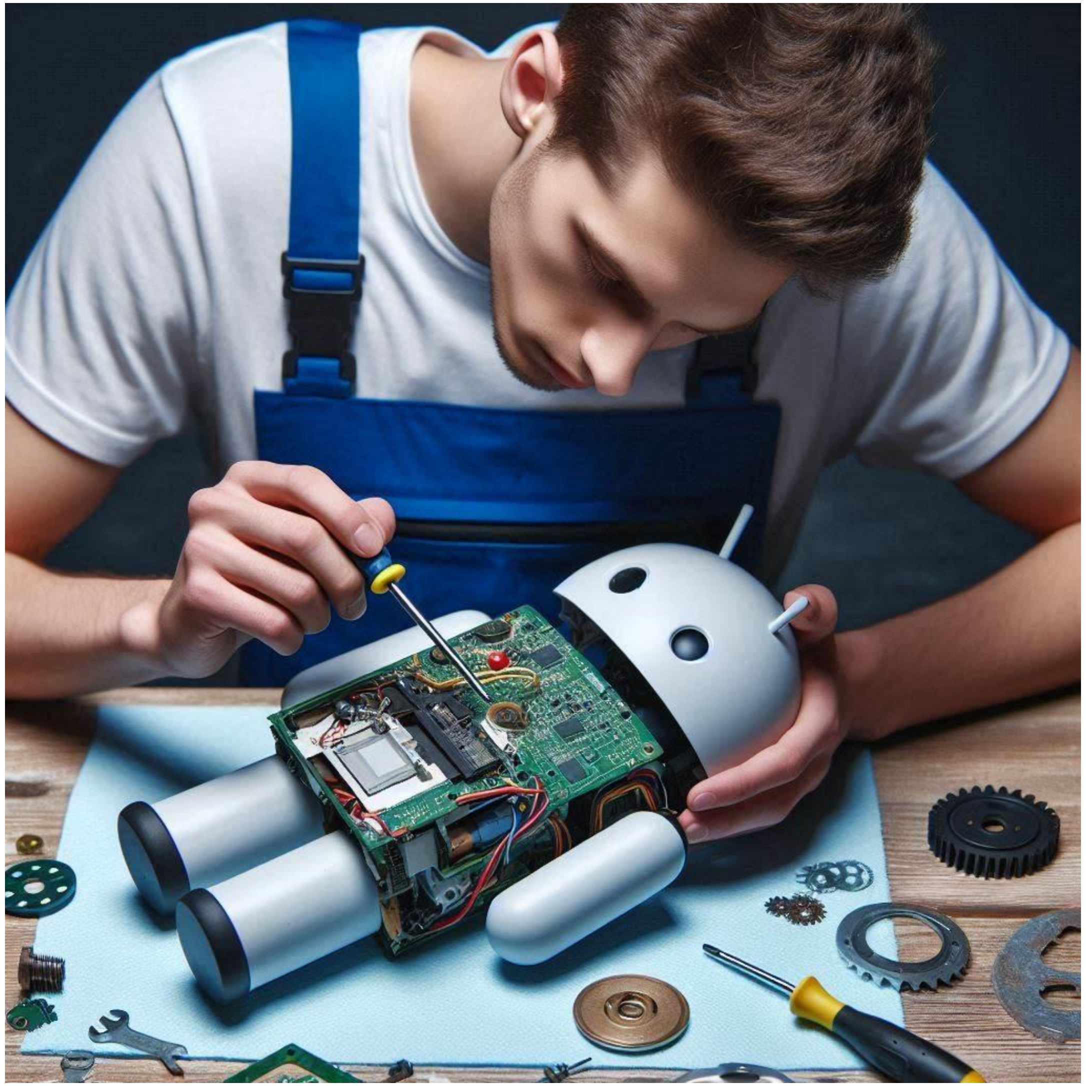
What the design flaws here?

1. Relying on cloud for essential features
   - Infrastructure might not last for the full product life
   - Key features should work with **local authentication** and ideally no mobile application
     - Local HTTP server for key settings
     - Public APIs
     - …
2. Exposing publicly the elements required for BLE communication
   - It saved us…
   - They cannot be changed

Doing the same for other IOT?

- One might believe it could be an interesting "business" but...
  - You need test devices
  - It took 8 months of work (so far)
  - We had luck
    - Other similar projects
    - Authentication flaw
  - Deploying at scale is a risky business
    - Need support
    - Need to handle all the exceptions

Instead of having to reverse, IOT should keep a minimal set of features independently of any 3rd party support. A bike should be functional without a 4G connection and a cloud infrastructure.



Picture generated by Microsoft Copilot

[TLP:GREEN]

Legal track – some hope?

1. European Commission directive 2024/1799 from 13th June 2024 (part of the Green Deal)
   - common rules promoting the repair of goods ("Right to Repair Directive")
   - Going into the right direction but not sufficient in this case…

Food for thought: is it really acceptable to purchase devices that could be "bricked" at any time for any reason?

Picture generated by Microsoft Copilot

[TLP:GREEN]

Conclusion

- ✓ The experience was fun, and our goals are reached (EV charger saved)
- ✓ As for any project, we faced issued, had a bit of luck and learned a lot.

But... It also raise many points

As professionals, hackers, passionate knowing that we should pay attention to the number of electronic wastes we produce

- Couldn't we design devices that could last?
- Shouldn't praise for open APIs for some key essential's features?
- Should the code be stored by an escrow in case of bankrupt?
- ...

We don't have a magic solution but feel that **something is wrong**.

Thanks!

Contacts:

- David Durvaux: @ddurvaux / david@autopsit.org
- Marc Durvaux: marc@autopsit.org
- Daniel Galinski: info@lookwatt.be

Thanks for SmartWatt (https://www.smartwatt.be/) for providing test devices!

Alternative implementations:

- Geert Meersman ESPHome project: https://github.com/geertmeersman/nexxtender
- nexxtender-ble: https://github.com/toSvenson/nexxtender-ble

Picture generated by Microsoft Copilot

[TLP:GREEN]