OTH REGENSBURG

# The persistent problems with cybersecurity: a negative example and an outlook on the Cyber Resilience Act

Sebastian Fischer (OTH Regensburg)

IARIA

ComputationWorld 2025 & DataSys 2025 - April 06 to April 10, 2025 - Valencia, Spain

# Prof. Dr. Sebastian Fischer

| | |
|---|---|
| *since 2023* | Professor for "Computer Science and System Security" at OTH Regensburg, Germany |
| *2021 - 2023* | Lecturer at OTH Regensburg, Germany |
| *2022* | Dr. rer. nat. at Freie Universität Berlin, Germany |
| *2018 - 2021* | Research Associate at Fraunhofer AISEC, Germany |
| *2015 - 2018* | Research Associate at OTH Regensburg, Germany |
| *2015* | M. Sc. Applied Research in Computer Science, OTH Regensburg |
| *2013* | B. Sc. Computer Science, OTH Regensburg |

sebastian.fischer@oth-regensburg.de

# Contents

- Missing API security
- **Example: Earl**
- Cyber Resilience Act (CRA)
- Conclusion / Outlook

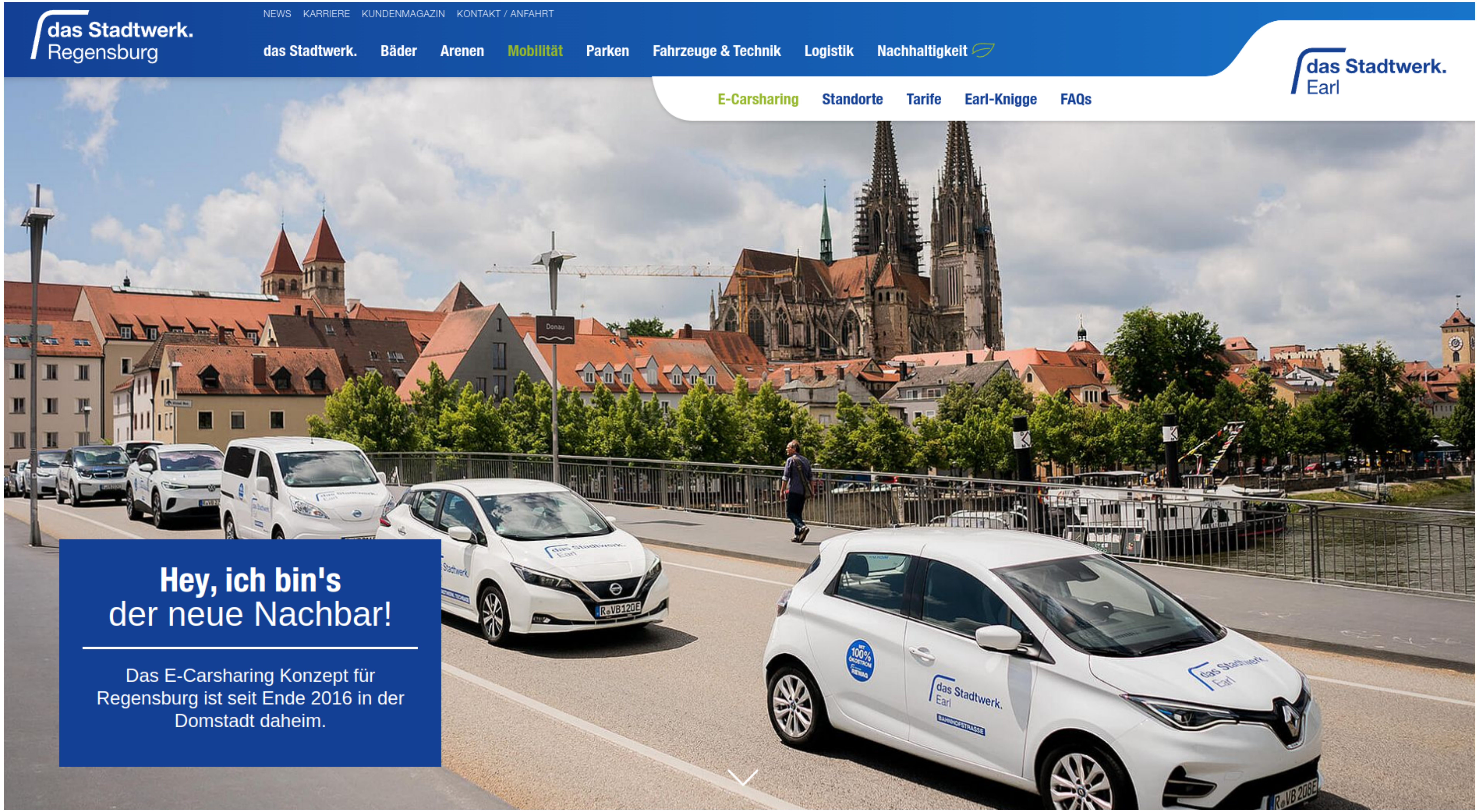
# Missing API security

- e.g. OWASP Top 10 API Security Risks – 2023
  - API1:2023 - Broken Object Level **Authorization**
  - API2:2023 - Broken **Authentication**
  - API3:2023 - Broken Object Property Level **Authorization**
  - API4:2023 - **Unrestricted** Resource Consumption
  - API5:2023 - Broken Function Level **Authorization**
- https://owasp.org/API-Security/editions/2023/en/0x11-t10/

# Work of Lea Laux

- **The following example with Earl is the work of Lea Laux!**
- Master student at OTH Regensburg
- Research on cybersecurity

# eCarsharing - Earl



**Hey, ich bin's**
der neue Nachbar!

Das E-Carsharing Konzept für Regensburg ist seit Ende 2016 in der Domstadt daheim.

# System of Earl

- Direct operation and billing by the municipal utility company Regensburg
- Application for managing the bookings: **fleetster** (earl.fleetster.de on the web, but also as an app for Android and iOS)
- RFID cards next to app for bookings
- Free charging with charging card in the vehicle charging card from REWAG
- Inverse Cloudboxx by **fleetster**: telematics, key management

# Contact

**Forschungskooperation IT-Sicherheit Earl-Fahrzeuge** 2 Messages

Quick Filter

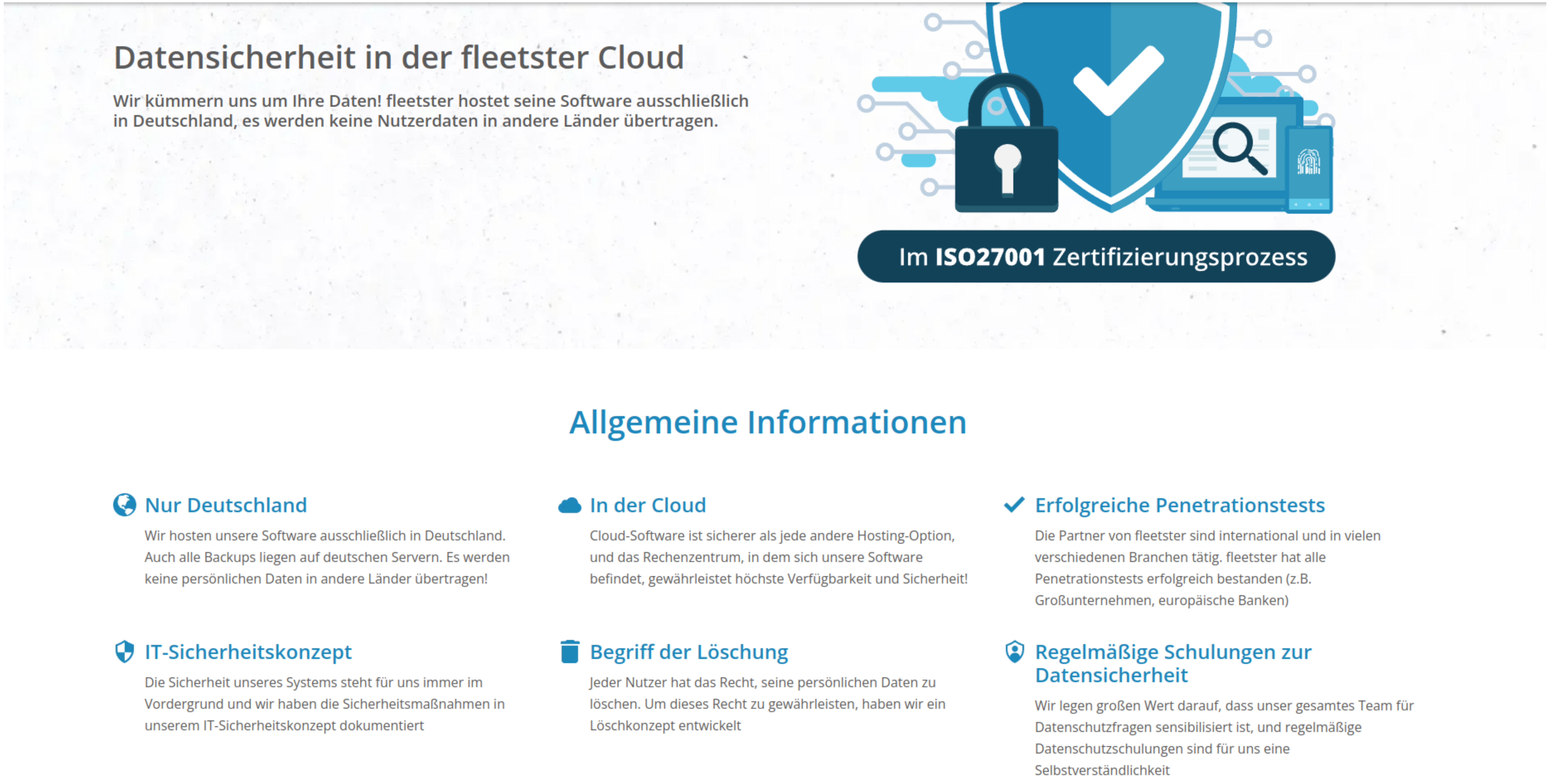
| Subject | Correspondents | Date | Location |
|---|---|---|---|
| Forschungskooperation IT-Sicherheit Earl-Fahrzeuge | → info@dasstadtwerk-earl.de | 13.08.23, 20:26 | Sent |
| Re: Forschungskooperation IT-Sicherheit Earl-Fahrzeuge | → info@dasstadtwerk-earl.de | 22.10.23, 11:05 | Sent |

- No response to mail after enquiry for research cooperation
- Telephone call: no interest or referral to fleetster

# fleetster?

- Self-description: Cloud software for modern fleets & mobility providers
- Marketing without interest in cooperation, because: **Security is a top priority here**

# fleetster?



## Datensicherheit in der fleetster Cloud

Wir kümmern uns um Ihre Daten! fleetster hostet seine Software ausschließlich in Deutschland, es werden keine Nutzerdaten in andere Länder übertragen.

Im **ISO27001** Zertifizierungsprozess

## Allgemeine Informationen

### Nur Deutschland

Wir hosten unsere Software ausschließlich in Deutschland. Auch alle Backups liegen auf deutschen Servern. Es werden keine persönlichen Daten in andere Länder übertragen!

### In der Cloud

Cloud-Software ist sicherer als jede andere Hosting-Option, und das Rechenzentrum, in dem sich unsere Software befindet, gewährleistet höchste Verfügbarkeit und Sicherheit!

### ✓ Erfolgreiche Penetrationstests

Die Partner von fleetster sind international und in vielen verschiedenen Branchen tätig. fleetster hat alle Penetrationstests erfolgreich bestanden (z.B. Großunternehmen, europäische Banken)

### IT-Sicherheitskonzept

Die Sicherheit unseres Systems steht für uns immer im Vordergrund und wir haben die Sicherheitsmaßnahmen in unserem IT-Sicherheitskonzept dokumentiert

### Begriff der Löschung

Jeder Nutzer hat das Recht, seine persönlichen Daten zu löschen. Um dieses Recht zu gewährleisten, haben wir ein Löschkonzept entwickelt

### Regelmäßige Schulungen zur Datensicherheit

Wir legen großen Wert darauf, dass unser gesamtes Team für Datenschutzfragen sensibilisiert ist, und regelmäßige Datenschutzschulungen sind für uns eine Selbstverständlichkeit

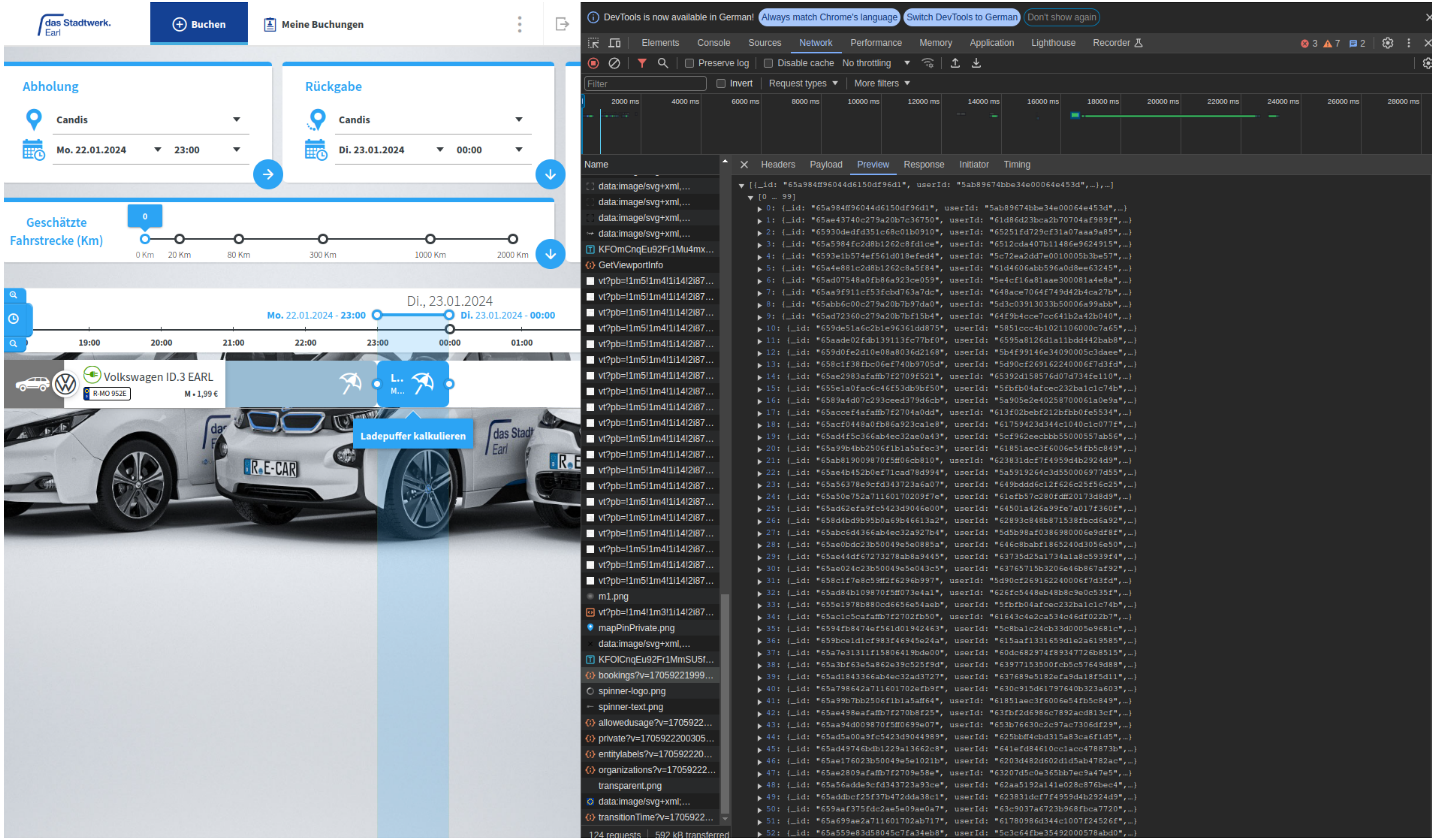
# Hacking rules

- Publicly findable information for more general Information (such as customers)
- For everything else: activated account (via the public utility company)
- Use of own user ID or user ID (and data) from friends
- Tests on own data or after permission from persons (if personal data)
- **Significant gaps now disclosed via Federal Office for Information Security (BSI) and fixed**

# Starting point

- URL: earl.fleetster.com
- Also available for: telekom, athlon, mikar, …
- Customers can also be found on the website, no secret / confidential information

# fleetster-API in the browser



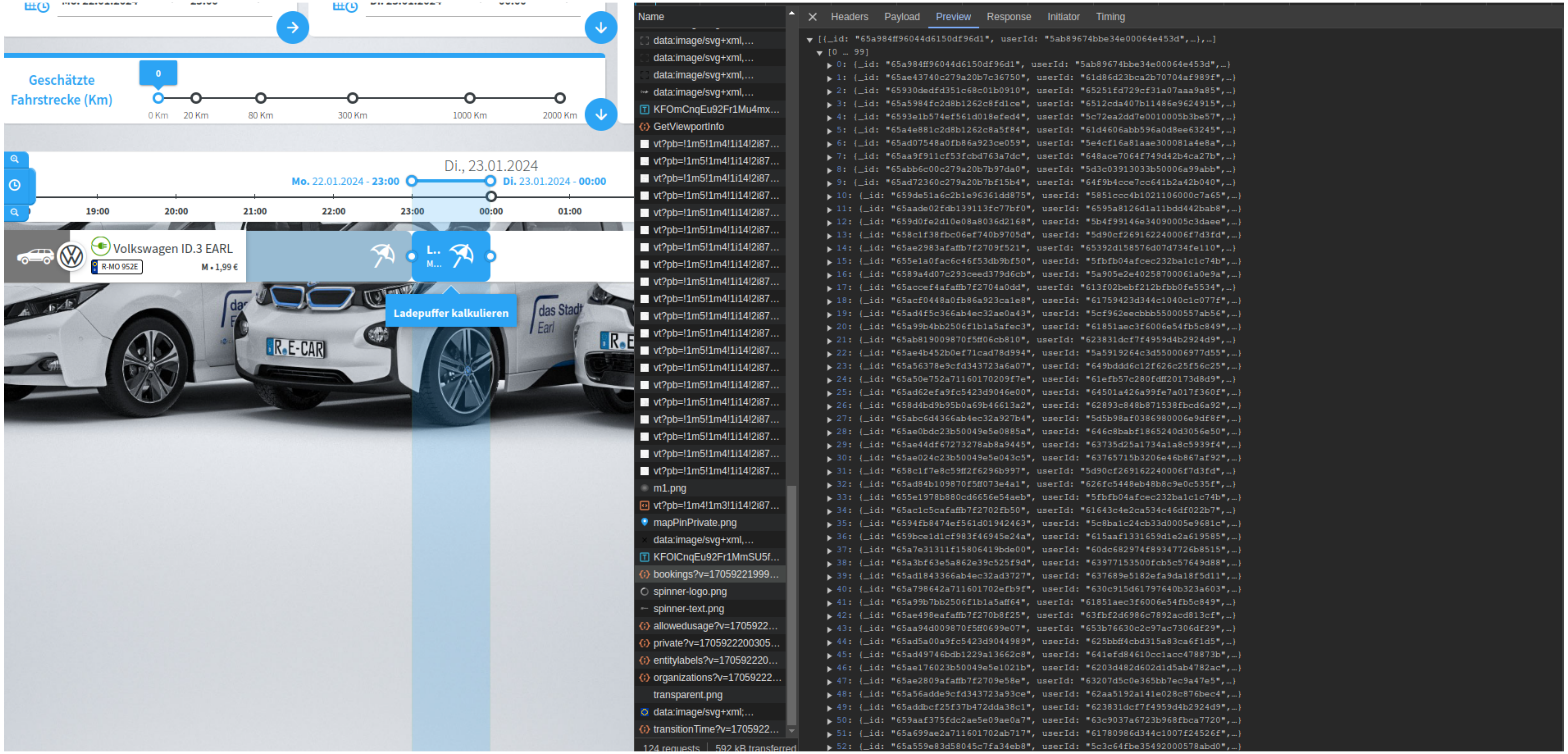
```
data:image/svg+xml,...
data:image/svg+xml,...
data:image/svg+xml,...
data:image/svg+xml,...
KFOmCnqEu92Fr1Mu4mx...
GetViewportInfo
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
m1.png
vt?pb=!1m4!1m3!1i14!2i87...
mapPinPrivate.png
data:image/svg+xml,...
KFOlCnqEu92Fr1MmSU5f...
bookings?v=17059221999...
spinner-logo.png
spinner-text.png
allowedusage?v=1705922...
private?v=1705922200305...
entitylabels?v=170592220...
organizations?v=17059222...
transparent.png
data:image/svg+xml;...
transitionTime?v=1705922...
124 requests | 592 kB transferred
```

```
▼ [{_id: "65a984ff96044d6150df96d1", userId: "5ab89674bbe34e00064e453d",…},…]
  ▼ [0 … 99]
    ▶ 0: {_id: "65a984ff96044d6150df96d1", userId: "5ab89674bbe34e00064e453d",…}
    ▶ 1: {_id: "65ae43740c279a20b7c36750", userId: "61d86d23bca2b70704af989f",…}
    ▶ 2: {_id: "65930dedfd351c68c01b0910", userId: "65251fd729cf31a07aaa9a85",…}
    ▶ 3: {_id: "65a5984fc2d8b1262c8fd1ce", userId: "6512cda407b11486e9624915",…}
    ▶ 4: {_id: "6593e1b574ef561d018efed4", userId: "5c72ea2dd7e0010005b3be57",…}
    ▶ 5: {_id: "65a4e881c2d8b1262c8a5f84", userId: "61d4606abb596a0d8ee63245",…}
    ▶ 6: {_id: "65ad07548a0fb86a923ce059", userId: "5e4cf16a81aae300081a4e8a",…}
    ▶ 7: {_id: "65aa9f911cf53fcbd763a7dc", userId: "648ace7064f749d42b4ca27b",…}
    ▶ 8: {_id: "65abb6c00c279a20b7b97da0", userId: "5d3c03913033b50006a99abb",…}
    ▶ 9: {_id: "65ad72360c279a20b7bf15b4", userId: "64f9b4cce7cc641b2a42b040",…}
    ▶ 10: {_id: "659de51a6c2b1e96361dd875", userId: "5851ccc4b1021106000c7a65",…}
    ▶ 11: {_id: "65aade02fdb139113fc77bf0", userId: "6595a8126d1a11bdd442bab8",…}
    ▶ 12: {_id: "659d0fe2d10e08a8036d2168", userId: "5b4f99146e34090005c3daee",…}
    ▶ 13: {_id: "658c1f38fbc06ef740b9705d", userId: "5d90cf26916224000 6f7d3fd",…}
    ▶ 14: {_id: "65ae2983afaffb7f2709f521", userId: "65392d158576d07d734fe110",…}
    ▶ 15: {_id: "655e1a0fac6c46f53db9bf50", userId: "5fbfb04afcec232ba1c1c74b",…}
    ▶ 16: {_id: "6589a4d07c293ceed379d6cb", userId: "5a905e2e40258700061a0e9a",…}
    ▶ 17: {_id: "65accef4afaffb7f2704a0dd", userId: "613f02bebf212bfbb0fe5534",…}
    ▶ 18: {_id: "65acf0448a0fb86a923ca1e8", userId: "61759423d344c1040c1c077f",…}
    ▶ 19: {_id: "65ad4f5c366ab4ec32ae0a43", userId: "5cf962eecbbb55000557ab56",…}
    ▶ 20: {_id: "65a99b4bb2506f1b1a5afec3", userId: "61851aec3f6006e54fb5c849",…}
    ▶ 21: {_id: "65ab819009870f5ff06cb810", userId: "623831dcf7f4959d4b2924d9",…}
    ▶ 22: {_id: "65ae4b452b0ef71cad78d994", userId: "5a5919264c3d550006977d55",…}
    ▶ 23: {_id: "65a56378e9cfd343723a6a07", userId: "649bddd6c12f626c25f56c25",…}
    ▶ 24: {_id: "65a50e752a71160170209f7e", userId: "61efb57c280fdff20173d8d9",…}
    ▶ 25: {_id: "65ad62efa9fc5423d9046e00", userId: "64501a426a99fe7a017f360f",…}
    ▶ 26: {_id: "658d4bd9b95b0a69b46613a2", userId: "62893c848b871538fbcd6a92",…}
    ▶ 27: {_id: "65abc6d4366ab4ec32a927b4", userId: "5d5b98af0386980006e9df8f",…}
    ▶ 28: {_id: "65ae0bdc23b50049e5e0885a", userId: "646c8babf1865240d3056e50",…}
    ▶ 29: {_id: "65ae44df67273278ab8a9445", userId: "63735d25a1734a1a8c5939f4",…}
    ▶ 30: {_id: "65ae024c23b50049e5e043c5", userId: "63765715b3206e46b867af92",…}
    ▶ 31: {_id: "658c1f7e8c59ff2f6296b997", userId: "5d90cf269162240006f7d3fd",…}
    ▶ 32: {_id: "65ad84b109870f5ff073e4a1", userId: "626fc5448eb48b8c9e0c535f",…}
    ▶ 33: {_id: "655e1978b880cd6656e54aeb", userId: "5fbfb04afcec232ba1c1c74b",…}
    ▶ 34: {_id: "65ac1c5cafaffb7f2702fb50", userId: "61643c4e2ca534c46df022b7",…}
    ▶ 35: {_id: "6594fb8474ef561d01942463", userId: "5c8ba1c24cb33d0005e9681c",…}
    ▶ 36: {_id: "659bce1d1cf983f46945e24a", userId: "615aaf1331659d1e2a619585",…}
    ▶ 37: {_id: "65a7e31311f15806419bde00", userId: "60dc682974f89347726b8515",…}
    ▶ 38: {_id: "65a3bf63e5a862e39c525f9d", userId: "63977153500fcb5c57649d88",…}
    ▶ 39: {_id: "65ad1843366ab4ec32ad3727", userId: "637689e5182efa9da18f5d11",…}
    ▶ 40: {_id: "65a798642a711601702efb9f", userId: "630c915d61797640b323a603",…}
    ▶ 41: {_id: "65a99b7bb2506f1b1a5aff64", userId: "61851aec3f6006e54fb5c849",…}
    ▶ 42: {_id: "65ae498eafaffb7f270b8f25", userId: "63fbf2d6986c7892acd813cf",…}
    ▶ 43: {_id: "65aa94d009870f5ff0699e07", userId: "653b76630c2c97ac7306df29",…}
    ▶ 44: {_id: "65ad5a00a9fc5423d9044989", userId: "625bbff4cbd315a83ca6f1d5",…}
    ▶ 45: {_id: "65ad49746bdb1229a13662c8", userId: "641efd84610cc1acc478873b",…}
    ▶ 46: {_id: "65ae176023b50049e5e1021b", userId: "6203d482d602d1d5ab4782ac",…}
    ▶ 47: {_id: "65ae2809afaffb7f2709e58e", userId: "63207d5c0e365bb7ec9a47e5",…}
    ▶ 48: {_id: "65a56adde9cfd343723a93ce", userId: "62aa5192a141e028c876bec4",…}
    ▶ 49: {_id: "65addbcf25f37b472dda38c1", userId: "623831dcf7f4959d4b2924d9",…}
    ▶ 50: {_id: "659aaf375fdc2ae5e09ae0a7", userId: "63c9037a6723b968fbca7720",…}
    ▶ 51: {_id: "65a699ae2a711601702ab717", userId: "61780986d344c1007f24526f",…}
    ▶ 52: {_id: "65a559e83d58045c7fa34eb8", userId: "5c3c64fbe3549200057 8abd0",…}
```

# fleetster-API in the browser

DevTools is now available in German! Always match Chrome's language Switch DevTools to German Don't show again

- Bookings to check whether there is a temporal overlap with booking period for selected filters exist:



```
data:image/svg+xml,...
data:image/svg+xml,...
data:image/svg+xml,...
data:image/svg+xml,...
KFOmCnqEu92Fr1Mu4mx...
GetViewportInfo
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
vt?pb=!1m5!1m4!1i14!2i87...
m1.png
vt?pb=!1m4!1m3!1i14!2i87...
mapPinPrivate.png
data:image/svg+xml,...
KFOlCnqEu92Fr1MmSU5f...
bookings?v=17059221999...
spinner-logo.png
spinner-text.png
allowedusage?v=1705922...
private?v=1705922200305...
entitylabels?v=170592220...
organizations?v=17059222...
transparent.png
data:image/svg+xml;...
transitionTime?v=1705922...
124 requests | 592 kB transferred
```

```
▼ [{_id: "65a984ff96044d6150df96d1", userId: "5ab89674bbe34e00064e453d",…},…]
  ▼ [0 … 99]
    ▶ 0: {_id: "65a984ff96044d6150df96d1", userId: "5ab89674bbe34e00064e453d",…}
    ▶ 1: {_id: "65ae43740c279a20b7c36750", userId: "61d86d23bca2b70704af989f",…}
    ▶ 2: {_id: "65930dedfd351c68c01b0910", userId: "65251fd729cf31a07aaa9a85",…}
    ▶ 3: {_id: "65a5984fc2d8b1262c8fd1ce", userId: "6512cda407b11486e9624915",…}
    ▶ 4: {_id: "6593e1b574ef561d018efed4", userId: "5c72ea2dd7e0010005b3be57",…}
    ▶ 5: {_id: "65a4e881c2d8b1262c8a5f84", userId: "61d4606abb596a0d8ee63245",…}
    ▶ 6: {_id: "65ad07548a0fb86a923ce059", userId: "5e4cf16a81aae300081a4e8a",…}
    ▶ 7: {_id: "65aa9f911cf53fcbd763a7dc", userId: "648ace7064f749d42b4ca27b",…}
    ▶ 8: {_id: "65abb6c00c279a20b7b97da0", userId: "5d3c03913033b50006a99abb",…}
    ▶ 9: {_id: "65ad72360c279a20b7bf15b4", userId: "64f9b4cce7cc641b2a42b040",…}
    ▶ 10: {_id: "659de51a6c2b1e96361dd875", userId: "5851ccc4b1021106000c7a65",…}
    ▶ 11: {_id: "65aade02fdb139113fc77bf0", userId: "6595a8126d1a11bdd442bab8",…}
    ▶ 12: {_id: "659d0fe2d10e08a8036d2168", userId: "5b4f99146e34090005c3daee",…}
    ▶ 13: {_id: "658c1f38fbc06ef740b9705d", userId: "5d90cf269162240006f7d3fd",…}
    ▶ 14: {_id: "65ae2983afaffb7f2709f521", userId: "65392d158576d07d734fe110",…}
    ▶ 15: {_id: "655e1a0fac6c46f53db9bf50", userId: "5fbfb04afcec232ba1c1c74b",…}
    ▶ 16: {_id: "6589a4d07c293ceed379d6cb", userId: "5a905e2e40258700061a0e9a",…}
    ▶ 17: {_id: "65accef4afaffb7f2704a0dd", userId: "613f02bebf212bfbb0fe5534",…}
    ▶ 18: {_id: "65acf0448a0fb86a923ca1e8", userId: "61759423d344c1040c1c077f",…}
    ▶ 19: {_id: "65ad4f5c366ab4ec32ae0a43", userId: "5cf962eecbbb55000557ab56",…}
    ▶ 20: {_id: "65a99b4bb2506f1b1a5afec3", userId: "61851aec3f6006e54fb5c849",…}
    ▶ 21: {_id: "65ab819009870f5ff06cb810", userId: "623831dcf7f4959d4b2924d9",…}
    ▶ 22: {_id: "65ae4b452b0ef71cad78d994", userId: "5a5919264c3d550006977d55",…}
    ▶ 23: {_id: "65a56378e9cfd343723a6a07", userId: "649bddd6c12f626c25f56c25",…}
    ▶ 24: {_id: "65a50e752a71160170209f7e", userId: "61efb57c280fdff20173d8d9",…}
    ▶ 25: {_id: "65ad62efa9fc5423d9046e00", userId: "64501a426a99fe7a017f360f",…}
    ▶ 26: {_id: "658d4bd9b95b0a69b46613a2", userId: "62893c848b871538fbcd6a92",…}
    ▶ 27: {_id: "65abc6d4366ab4ec32a927b4", userId: "5d5b98af0386980006e9df8f",…}
    ▶ 28: {_id: "65ae0bdc23b50049e5e0885a", userId: "646c8babf1865240d3056e50",…}
    ▶ 29: {_id: "65ae44df67273278ab8a9445", userId: "63735d25a1734a1a8c5939f4",…}
    ▶ 30: {_id: "65ae024c23b50049e5e043c5", userId: "63765715b3206e46b867af92",…}
    ▶ 31: {_id: "658c1f7e8c59ff2f6296b997", userId: "5d90cf269162240006f7d3fd",…}
    ▶ 32: {_id: "65ad84b109870f5ff073e4a1", userId: "626fc5448eb48b8c9e0c535f",…}
    ▶ 33: {_id: "655e1978b880cd6656e54aeb", userId: "5fbfb04afcec232ba1c1c74b",…}
    ▶ 34: {_id: "65ac1c5cafaffb7f2702fb50", userId: "61643c4e2ca534c46df022b7",…}
    ▶ 35: {_id: "6594fb8474ef561d01942463", userId: "5c8ba1c24cb33d0005e9681c",…}
    ▶ 36: {_id: "659bce1d1cf983f46945e24a", userId: "615aaf1331659d1e2a619585",…}
    ▶ 37: {_id: "65a7e31311f15806419bde00", userId: "60dc682974f89347726b8515",…}
    ▶ 38: {_id: "65a3bf63e5a862e39c525f9d", userId: "63977153500fcb5c57649d88",…}
    ▶ 39: {_id: "65ad1843366ab4ec32ad3727", userId: "637689e5182efa9da18f5d11",…}
    ▶ 40: {_id: "65a798642a711601702efb9f", userId: "630c915d61797640b323a603",…}
    ▶ 41: {_id: "65a99b7bb2506f1b1a5aff64", userId: "61851aec3f6006e54fb5c849",…}
    ▶ 42: {_id: "65ae498eafaffb7f270b8f25", userId: "63fbf2d6986c7892acd813cf",…}
    ▶ 43: {_id: "65aa94d009870f5ff0699e07", userId: "653b76630c2c97ac7306df29",…}
    ▶ 44: {_id: "65ad5a00a9fc5423d9044989", userId: "625bbff4cbd315a83ca6f1d5",…}
    ▶ 45: {_id: "65ad49746bdb1229a13662c8", userId: "641efd84610cc1acc478873b",…}
    ▶ 46: {_id: "65ae176023b50049e5e1021b", userId: "6203d482d602d1d5ab4782ac",…}
    ▶ 47: {_id: "65ae2809afaffb7f2709e58e", userId: "63207d5c0e365bb7ec9a47e5",…}
    ▶ 48: {_id: "65a56adde9cfd343723a93ce", userId: "62aa5192a141e028c876bec4",…}
    ▶ 49: {_id: "65addbcf25f37b472dda38c1", userId: "623831dcf7f4959d4b2924d9",…}
    ▶ 50: {_id: "659aaf375fdc2ae5e09ae0a7", userId: "63c9037a6723b968fbca7720",…}
    ▶ 51: {_id: "65a699ae2a711601702ab717", userId: "61780986d344c1007f24526f",…}
    ▶ 52: {_id: "65a559e83d58045c7fa34eb8", userId: "5c3c64fbe3549200057 8abd0",…}
```

# cURL / HTTP Requests

- Communication in web applications via HTTP Requests / response and REST

- Requests can generally not only be executed via browser

  - ⇒ Client: cURL (command line)

- Next: View of requests with Authorisation header from active client session

# cURL request

```
curl https://earl.fleetster.de/bookings?v=1699555681898
&endDate%5B%24gte%5D=2023-11-09T18%3A48%3A01.897Z
&fields%5B%5D=type
&fields%5B%5D=locationStartId
&fields%5B%5D=locationEndId
&fields%5B%5D=state
&fields%5B%5D=stops
&fields%5B%5D=startDate
&fields%5B%5D=endDate
&fields%5B%5D=vehicleId
&fields%5B%5D=userId
&fields%5B%5D=extended.BikeSharing
&fields%5B%5D=extended.CostCenter
&fields%5B%5D=extended.Vouchers
&fields%5B%5D=modified
&fields%5B%5D=buffer
&state%5B%24nin%5D%5B%5D=expired
&state%5B%24nin%5D%5B%5D=canceled
```

# Response

```
[
  {
    "_id": "57da8bc3d65cc70500ec103b",
    "userId": "57da8bc3d65cc70500ec103b",
    "vehicleId": "57da8bc3d65cc70500ec103b",
    "companyId": "57da8bc3d65cc70500ec103b",
    "startDate": "2018-02-14T09:00:00.000Z",
    "endDate": "2018-02-14T11:00:00.000Z",
    "initialStartDate": "2018-02-14T09:00:00.000Z",
    "initialEndDate": "2018-02-14T11:00:00.000Z",
    "locationStartId": "57da8bc3d65cc70500ec103b",
    "locationEndId": "57da8bc3d65cc70500ec103b",
    "type": "private",
    "state": "canceled",
    "extended": {},
    "deleted": true,
    "estimatedDistance": 25,
    "startMileage": 1337,
```

# Response

- Result: List of booking objects - with all essential information

- Provides too much information: not all data on other bookings necessary to determine whether the vehicle is free at a given time and has sufficient capacity

- Resulting idea: What happens without filters?

# GET request without filters

- curl https://earl.fleetster.de/bookings? … > earldata.json

- stat -c "%s %n" -- earldata.json

- 154916452 earldata.json

# GET request without filters

- curl https://earl.fleetster.de/bookings? … > earldata.json
- stat -c "%s %n" -- earldata.json
- 154916452 earldata.json

- **JSON file with all bookings since 2016 (start of Earl)**
- **150 MB data with IDs for users, vehicles, locations, ...**

# Data

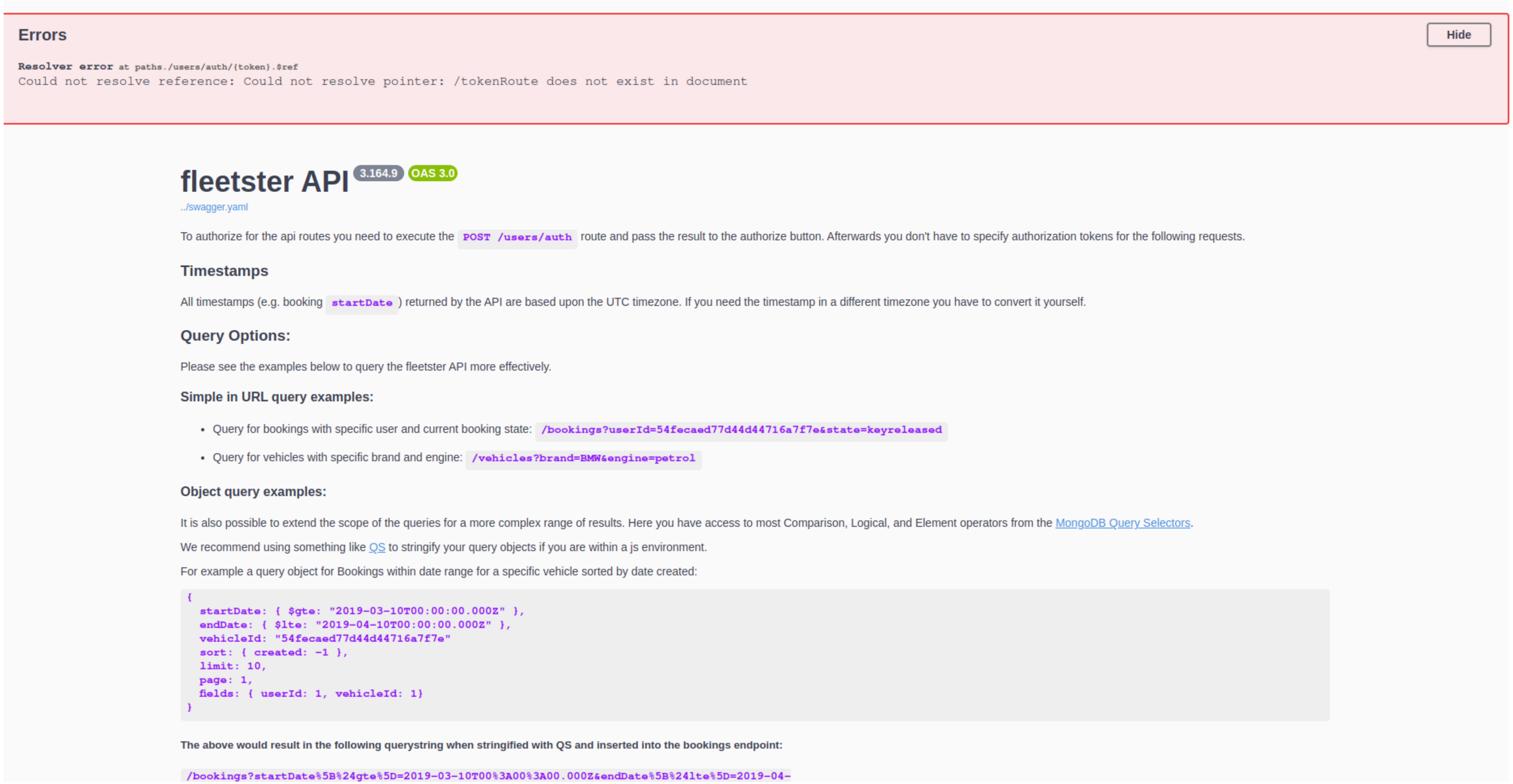
```
      userId duration                     cost
2402  0      0 days 00:02:00              -3.00
2893  1      0 days 00:44:00              -3.00
2026  2      34 days 04:41:00             0.00
...
464   7      104 days 19:57:03.995000  15706.77
308   8      301 days 01:20:40.259000  17317.37
16    9      205 days 18:38:24.209000  17597.73
```

Additional: internal vehicle functions, like suspiciousVehicleActivityLastWarning

# Data from user

- Destinations (places, plans, names, exact addresses if applicable)
- Purpose of the vehicle (destinations, goods transported, passenger transport, ...)
- Error messages, complaints (cleanliness, charging status, ...)
- Support requests (redemption of bonus points from other programmes, longer messages including names)
- Accident documentation (course of events, damage)

# System for managing bookings (API)



Errors

```
Resolver error at paths./users/auth/{token}.$ref
Could not resolve reference: Could not resolve pointer: /tokenRoute does not exist in document
```

fleetster API 3.164.9 OAS 3.0

../swagger.yaml

To authorize for the api routes you need to execute the `POST /users/auth` route and pass the result to the authorize button. Afterwards you don't have to specify authorization tokens for the following requests.

Timestamps

All timestamps (e.g. booking `startDate`) returned by the API are based upon the UTC timezone. If you need the timestamp in a different timezone you have to convert it yourself.

Query Options:

Please see the examples below to query the fleetster API more effectively.

Simple in URL query examples:

- Query for bookings with specific user and current booking state: `/bookings?userId=54fecaed77d44d44716a7f7e&state=keyreleased`
- Query for vehicles with specific brand and engine: `/vehicles?brand=BMW&engine=petrol`

Object query examples:

It is also possible to extend the scope of the queries for a more complex range of results. Here you have access to most Comparison, Logical, and Element operators from the MongoDB Query Selectors.

We recommend using something like QS to stringify your query objects if you are within a js environment.

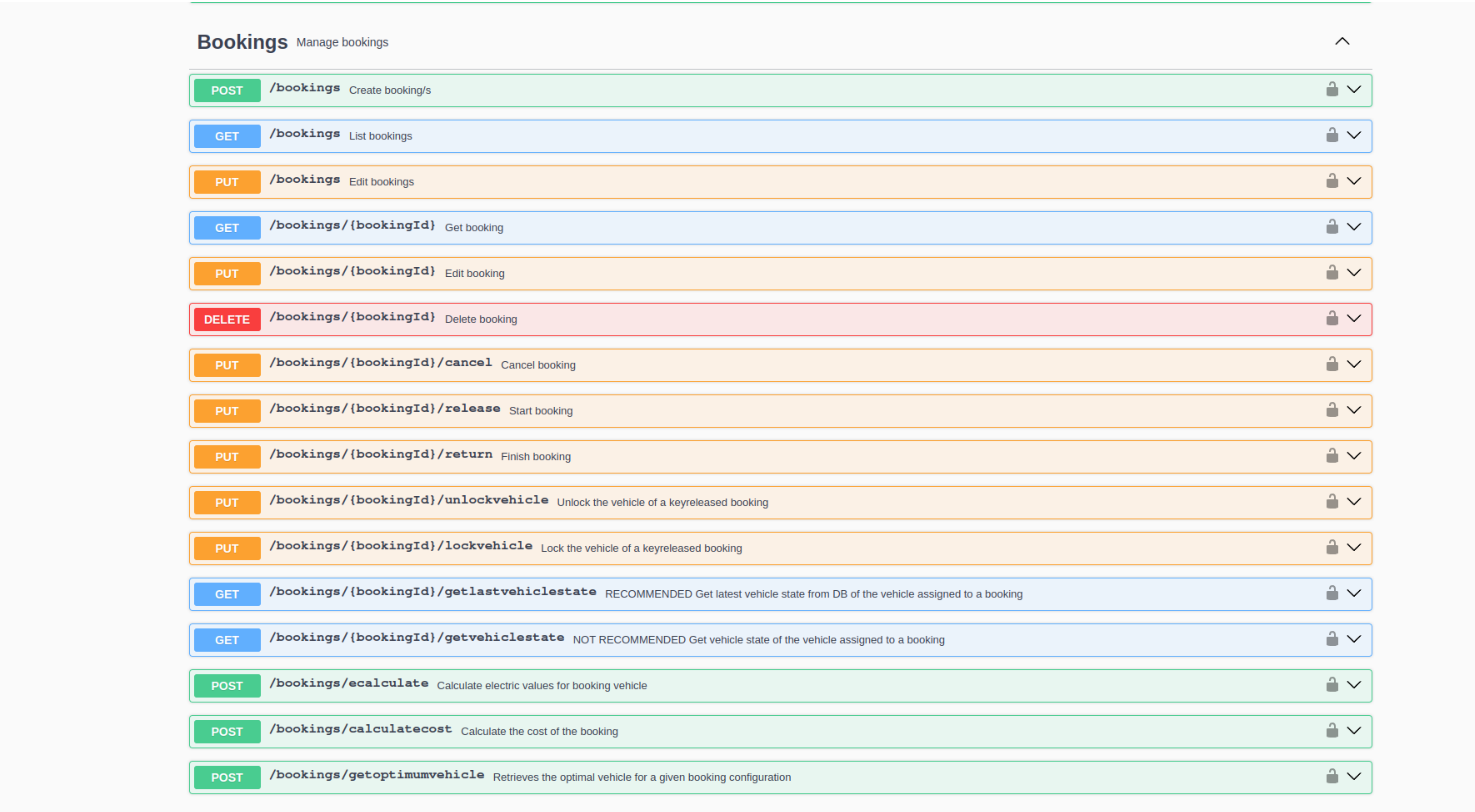
For example a query object for Bookings within date range for a specific vehicle sorted by date created:

```
{
  startDate: { $gte: "2019-03-10T00:00:00.000Z" },
  endDate: { $lte: "2019-04-10T00:00:00.000Z" },
  vehicleId: "54fecaed77d44d44716a7f7e"
  sort: { created: -1 },
  limit: 10,
  page: 1,
  fields: { userId: 1, vehicleId: 1}
}
```

**The above would result in the following querystring when stringified with QS and inserted into the bookings endpoint:**

```
/bookings?startDate%5B%24gte%5D=2019-03-10T00%3A00%3A00.000Z&endDate%5B%24lte%5D=2019-04-
```

# System for managing bookings (API)



**Bookings** Manage bookings

POST `/bookings` Create booking/s

GET `/bookings` List bookings

PUT `/bookings` Edit bookings

GET `/bookings/{bookingId}` Get booking

PUT `/bookings/{bookingId}` Edit booking

DELETE `/bookings/{bookingId}` Delete booking

PUT `/bookings/{bookingId}/cancel` Cancel booking

PUT `/bookings/{bookingId}/release` Start booking

PUT `/bookings/{bookingId}/return` Finish booking

PUT `/bookings/{bookingId}/unlockvehicle` Unlock the vehicle of a keyreleased booking

PUT `/bookings/{bookingId}/lockvehicle` Lock the vehicle of a keyreleased booking

GET `/bookings/{bookingId}/getlastvehiclestate` RECOMMENDED Get latest vehicle state from DB of the vehicle assigned to a booking

GET `/bookings/{bookingId}/getvehiclestate` NOT RECOMMENDED Get vehicle state of the vehicle assigned to a booking

POST `/bookings/ecalculate` Calculate electric values for booking vehicle

POST `/bookings/calculatecost` Calculate the cost of the booking

POST `/bookings/getoptimumvehicle` Retrieves the optimal vehicle for a given booking configuration

# Selected endpoints

- GET /bookings: bereits gezeigt
- POST /bookings
- PUT /bookings(/{bookingId})
- POST /bookings/calculatecost
- GET /locations
- GET /publicLocations/{adminGroup}
- GET /vehicles
- GET /vehicles/vehicleId

# POST /bookings/calculatecost

- Idea: Calculation of the expected costs of a booking
- Parameters: Booking ID, user ID, vehicle ID, start, end
- Expected response: Cost of the booking

# POST /bookings/calculatecost

- Idea: Calculation of the expected costs of a booking
- Parameters: Booking ID, user ID, vehicle ID, start, end
- Expected response: Cost of the booking
- Actual response: Cost of the booking

# POST /bookings/calculatecost

- Idea: Calculation of the expected costs of a booking
- Parameters: Booking ID, user ID, vehicle ID, start, end
- Expected response: Cost of the booking
- Actual response: Cost of the booking **and all data of the person with associated ID**

# User data

- General information: **Name, address, date and place of birth, nationality**
- Discount-specific information: RVV subscription number, REWAG customer number, RKom customer number, student number
- Internal information on Earl use: RFID card number, timestamp of registration confirmation, last login, last password change, ...
- **Direct debit mandate (if issued): IBAN, BIC, ...**

# Results…

- calculatecost harmless, as long as no user ID is available…
- …but we have all the IDs of all users who have ever made a booking from the bookings endpoint…

# Locations endpoint

- locations endpoint for all available locations in the current system, no secret data per se, only internal data like created or modified timestamp

- GET /publicLocations/{adminGroup} for locations any customer of fleetster

  - yes, also with authorisation header from Earl…

- Customers? telekom, athlon, mikar…

  ```
  stat -c "%s %n" -- telekom_locations.json
  72692 telekomlocations.json
  stat -c "%s %n" -- athlon_locations.json
  25508 athlon_locations.json
  stat -c "%s %n" -- mikar_locations.json
  149324 mikar_locations.json
  ```

# Vehicle endpoint

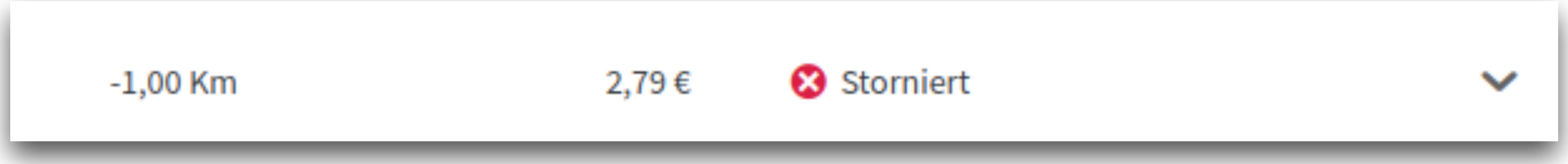
- All available vehicles for users via vehicles
- For respective ID corresponding to vehicle endpoint with vehicles/{vehicleId}
- Internal information for vehicle: Mileage, Information on the activation of mail notifications for certain events, user IDs for service trips, ...
  - ⇒ no secret data, misuse nevertheless possible

# Car bookings

- Book with an unauthorised user ID: **unauthorised**
- Own bookings: cancellation of bookings, changes to start and end times, kilometres, …
- **Show potential: Change booking so that amount to be paid changes**
- Change to own disadvantage

# Car bookings

- -1.00 km travelled



-1,00 Km 2,79 € ☒ Storniert

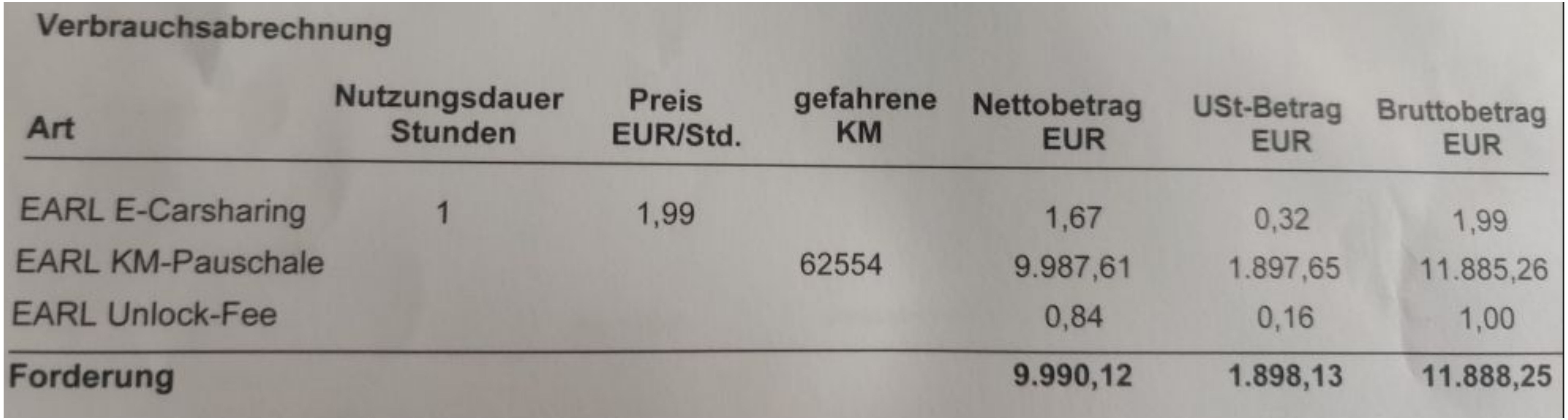
- Gets canceled later

# Invoice

- Billing period: per quarter
- Payment: bank transfer or direct debit
- Consequence of billing period: Results on invoice only at the end of the quarter
- **Automated processing**

# Invoice

- 11 888 Euro for 62 554 km **in one hour**



Verbrauchsabrechnung

| Art | Nutzungsdauer Stunden | Preis EUR/Std. | gefahrene KM | Nettobetrag EUR | USt-Betrag EUR | Bruttobetrag EUR |
|---|---|---|---|---|---|---|
| EARL E-Carsharing | 1 | 1,99 | | 1,67 | 0,32 | 1,99 |
| EARL KM-Pauschale | | | 62554 | 9.987,61 | 1.897,65 | 11.885,26 |
| EARL Unlock-Fee | | | | 0,84 | 0,16 | 1,00 |
| **Forderung** | | | | **9.990,12** | **1.898,13** | **11.888,25** |

# Summary

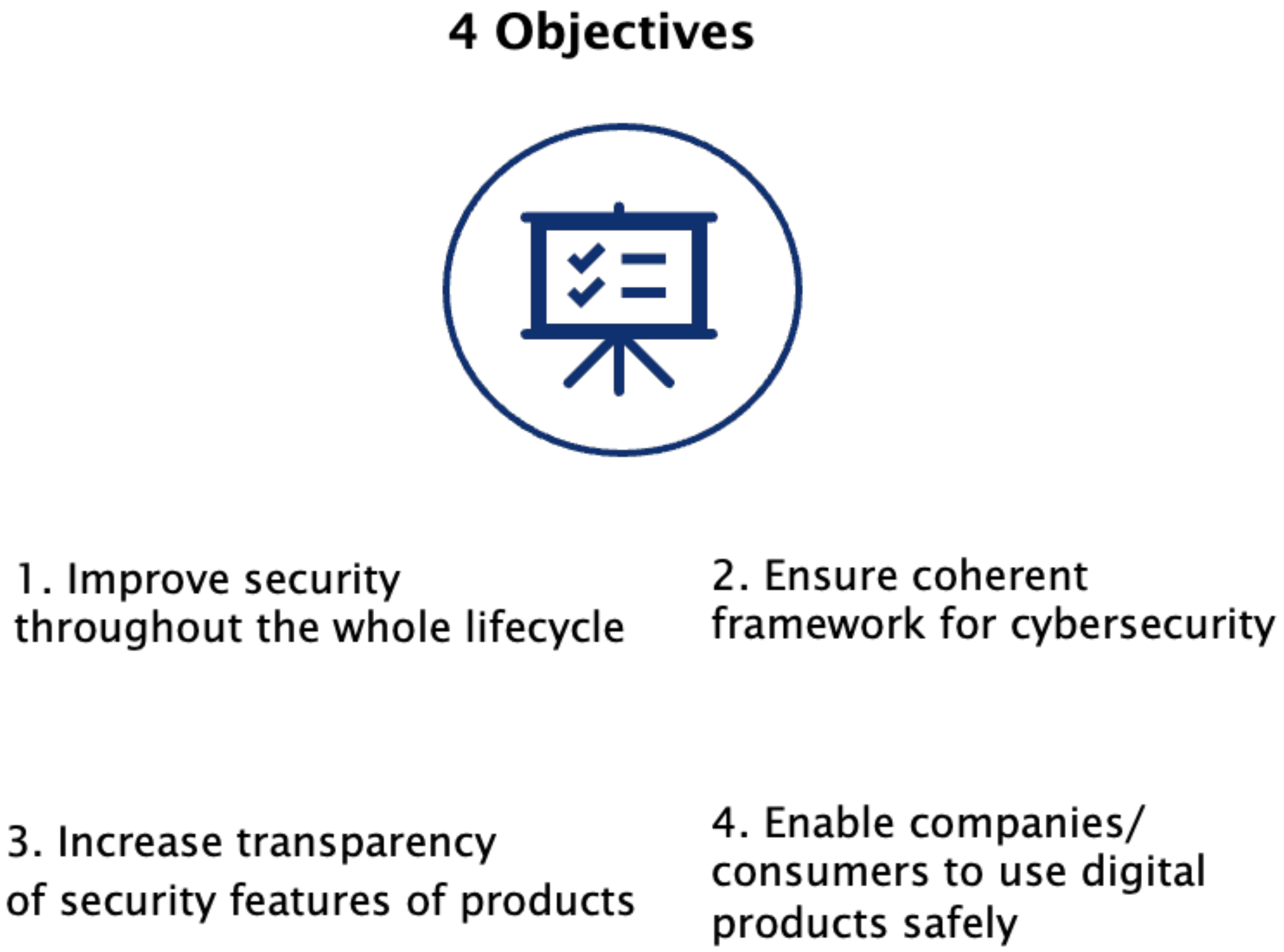
- All bookings since the start of Earl
- Possibility to get all the private data from any customer over the /bookings/calculatecost endpoint
- Change own bookings (also afterwards) without checks

# Responsible Disclosure

- Notification and coordination of the disclosure process via Federal Office for Information Security
- Initial disclosure: 11.12.2023
- 11.01.2024 Request for current status
- 15.01.2024 BSI feedback and confirmation that Vulnerability still exists
- **Mid-May until patch**

# Cyber Resilience Act (CRA)

- Introduces new mandatory cybersecurity requirements for hardware and software products throughout the whole lifecycle
- Regulation focuses on products with digital elements
- Classification of products into different classes + exclusion criteria



**4 Objectives**

1. Improve security throughout the whole lifecycle

2. Ensure coherent framework for cybersecurity

3. Increase transparency of security features of products

4. Enable companies/ consumers to use digital products safely

# Challenges for manufacturers of IoT products

- How to define requirements for a software that could assists manufacturers with complying with the CRA?
- Additional overhead for manufacturers to proof compliance
- How can compliance be proven to a third party?

?

# Solutions we are working on

- Research Question: How could a software prototype look like, that assists manufacturers with vulnerability detection to comply with the CRA?

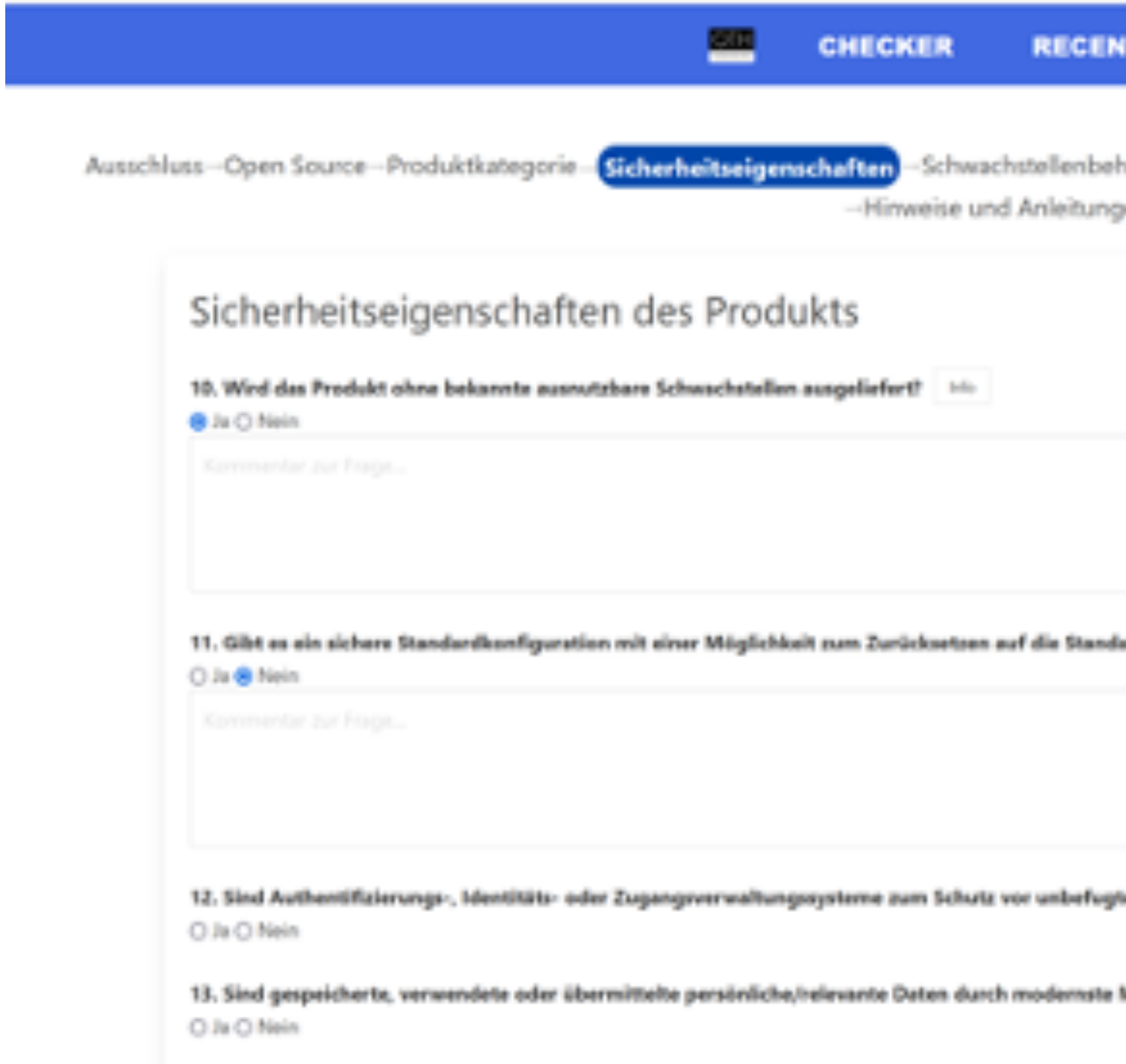
- Idea: Introducing Software that performs compliance checks for IoT devices

☑ CRA Compliance Checklist

☑ Vulnerability Scanner

# CRA Compliance Checklist

- A tool to determine the current cyber security standard and to monitor compliance with the requirements of the Cyber Resiliance Act
- Documentation on the current status and the degree of compliance with the regulation
- Tips and information on compliance with the requirements



Sicherheitseigenschaften des Produkts

**10. Wird das Produkt ohne bekannte ausnutzbare Schwachstellen ausgeliefert?**

● Ja ○ Nein

Kommentar zur Frage...

**11. Gibt es ein sichere Standardkonfiguration mit einer Möglichkeit zum Zurücksetzen auf die Standa**

○ Ja ● Nein

Kommentar zur Frage...

**12. Sind Authentifizierungs-, Identitäts- oder Zugangsverwaltungsysteme zum Schutz vor unbefugt**

○ Ja ○ Nein

**13. Sind gespeicherte, verwendete oder übermittelte persönliche/relevante Daten durch modernste**

○ Ja ○ Nein

# Conclusion / Outlook

- Cybersecurity is important…
- It is still ignored (see fleetster)
- One possible solution: regulations
    - => Cyber Resilience Act

# References

[1] R. Lemos, “Security Guru: Let’s Secure the Net,” 2024, [Online; accessed: 2024-02-27]. URL https://www.zdnet.com/article/security-guru-lets-secure-the-net/

[2] S. Ahmed, M. Carr, M. Nouh, and J. Merritt, “State of the Connected World,” Tech. rep., World Economic Forum, Jan. 2023.

[3] European Commission, “Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020,” 2022, [Online; accessed: 2024-02-27]. URL https://eur- lex.europa.eu/legal- content/ENTXT/?uri=celex: 52022PC0454

[4] C. Skouloudi, A. Malatras, R. Naydenov, and G. Dede, “Guidelines for Securing the Internet of Things,” Tech. rep., ENISA, 2020.

[5] ENISA, “Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures,” Tech. rep., European Union Agency For Network And Information Security, Nov. 2017.

[6] J. P. Castellanos Ardila, B. Gallina, and F. Ul Muram, “Compliance Checking of Software Processes: A Systematic Literature Review,” Journal of Software: Evolution and Process, 34(5), p. e2440, 2022, ISSN 2047-7481, doi:10.1002/smr.2440.

[7] M. Barati, G. Theodorakopoulos, and O. Rana, “Automating GDPR Compliance Verification for Cloud-hosted Services,” in 2020 Inter- national Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6, Oct. 2020, doi:10.1109/ISNCC49221.2020.9297309.

[8] J. F. Car´ıas, S. Arrizabalaga, L. Labaka, and J. Hernantes, “Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs,” IEEE Access, 9, pp. 80741–80762, 2021, ISSN 2169-3536, doi:10.1109/ACCESS.2021. 3085530.

[9] RiskOptics, “RZenGRC,” 2024, [Online; accessed: 2024-02-27]. URL https://reciprocity.com/product/zengrc/

[10] cloudsmith, “cloud native artifact management,” 2024, [Online; ac- cessed: 2024-02-27].
URL https://cloudsmith.com/product/cloud-native-artifact-management

[11] F. Lombardi and A. Fanton, “From DevOps to DevSecOps Is Not Enough. CyberDevOps: An Extreme Shifting-Left Architecture to Bring Cybersecurity within Software Security Lifecycle Pipeline,” Software Quality Journal, 31(2), pp. 619–654, Jun. 2023, ISSN 1573-1367, doi: 10.1007/s11219- 023- 09619- 3.

[12] “Vue.Js,” 2024, [Online; accessed: 2024-02-27]. URL https://vuejs.org/

[13] “Git,” 2024, [Online; accessed: 2024-02-27]. URL https://git-scm.com/

[14] “Anchore/Syft,” Anchore, Inc., Jan. 2024.

[15] “Semgrep — Find Bugs and Enforce Code Standards,” 2024, [Online; accessed: 2024-02-27]. URL https://semgrep.dev/

[16] “Flawfinder Home Page,” 2024, [Online; accessed: 2024-02-27]. URL https://dwheeler.com/flawfinder/

[17] “Cppcheck - A Tool for Static C/C++ Code Analysis,” 2024, [Online; accessed: 2024-02-27]. URL https://cppcheck.sourceforge.io/

[18] “Horusec,” 2024, [Online; accessed: 2024-02-27]. URL https://horusec.io/site/

[19] “Docker: Accelerated Container Application Development,” May 2022, [Online; accessed: 2024-02-27]. URL https://www.docker.com/

[20] “GitHub:Let’sBuildfromHere,”2024,[Online;accessed:2024-02-27]. URL https://github.com/

[21] S. Inc, “Sonatype OSS Index,” 2024, [Online; accessed: 2024-02-27]. URL https://ossindex.sonatype.org/

[22] C.Gentsch,“EvaluationofOpenSourceStaticAnalysisSecurityTesting (SAST) Tools for C,” Technical Report DLR-IB-DW-JE-2020-16, DLR German Aerospace Center, Jan. 2020.

[23] National Institute for Standards and Technology, “Juliet C/C++ 1.3 - NIST Software Assurance Reference Dataset,” 2017, [Online; accessed: 2024-02-27].URL https://samate.nist.gov/SARD/test-suites/112

[24] National Institute for Standards and Technology, “Wireshark 1.8.0 - NIST Software Assurance Reference Dataset,” 2014, [Online; accessed: 2024-02-27].URL https://samate.nist.gov/SARD/test-suites/94

[25] D. A. Wheeler, “Flawfinder/Flawfinder.Py at Master · David- a-Wheeler/Flawfinder · GitHub,” https://github.com/david-a- wheeler/flawfinder/blob/master/flawfinder.py.

[26] “Semgrep-Rules/c/Lang/Security at Develop · Semgrep/Semgrep- Rules · GitHub,” https://github.com/semgrep/semgrep- rules/tree/develop/c/lang/security.