On Trusting Third-party Satellite Data

Sean Crosby (author and presenter)

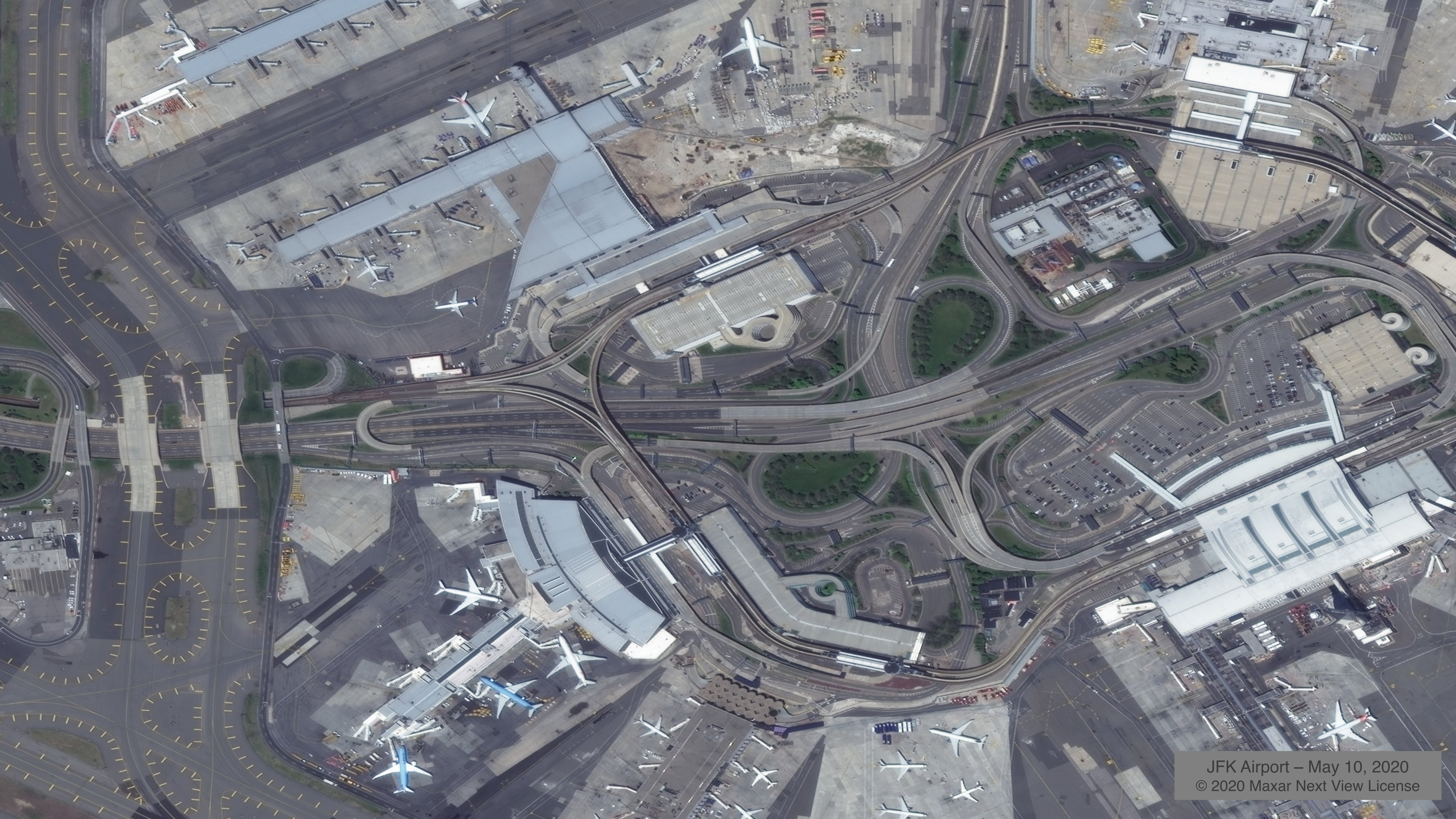
Kurt Brenning (co-author)

36th Annual Small Satellite Conference 2022

Logan, Utah

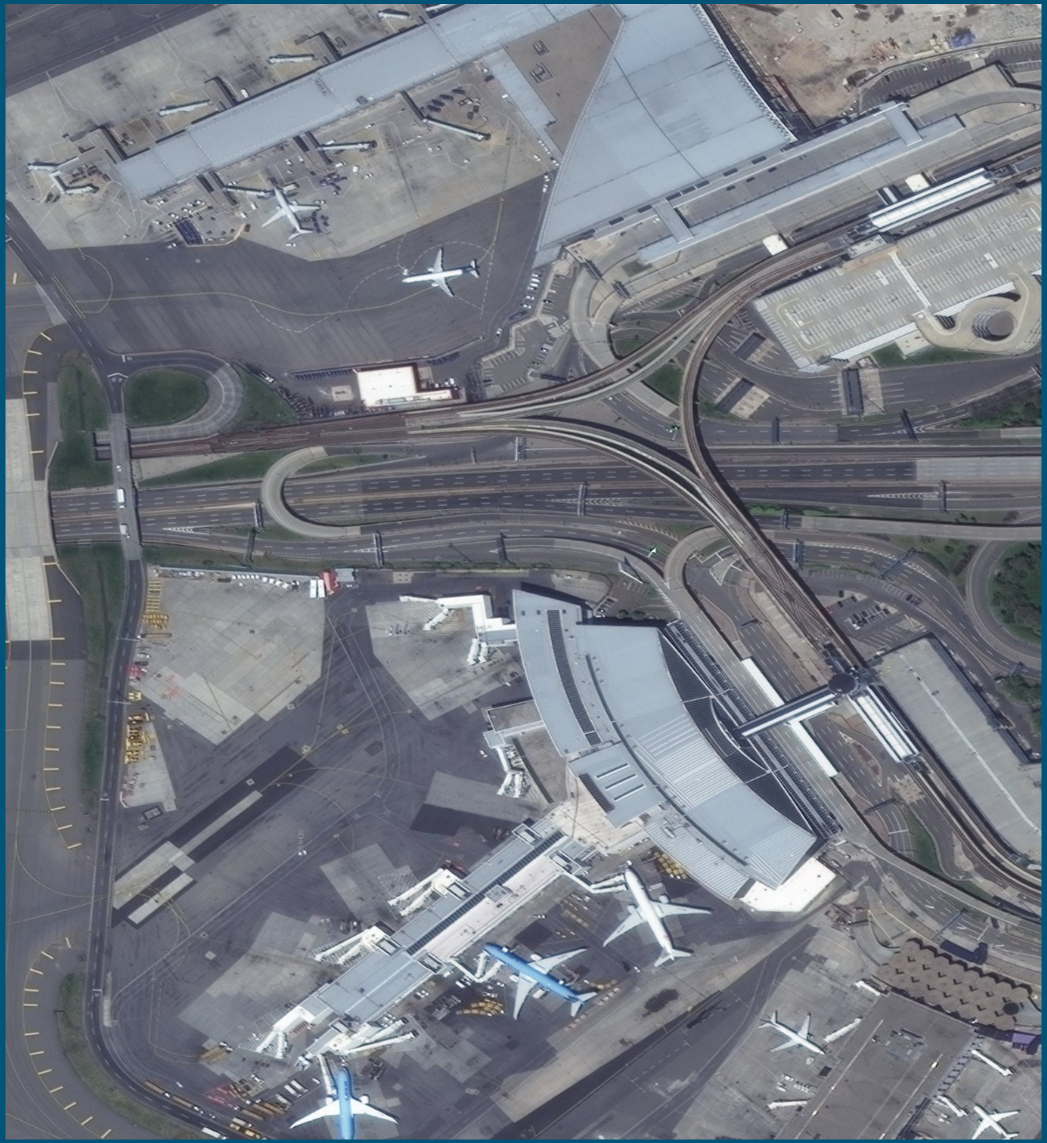
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

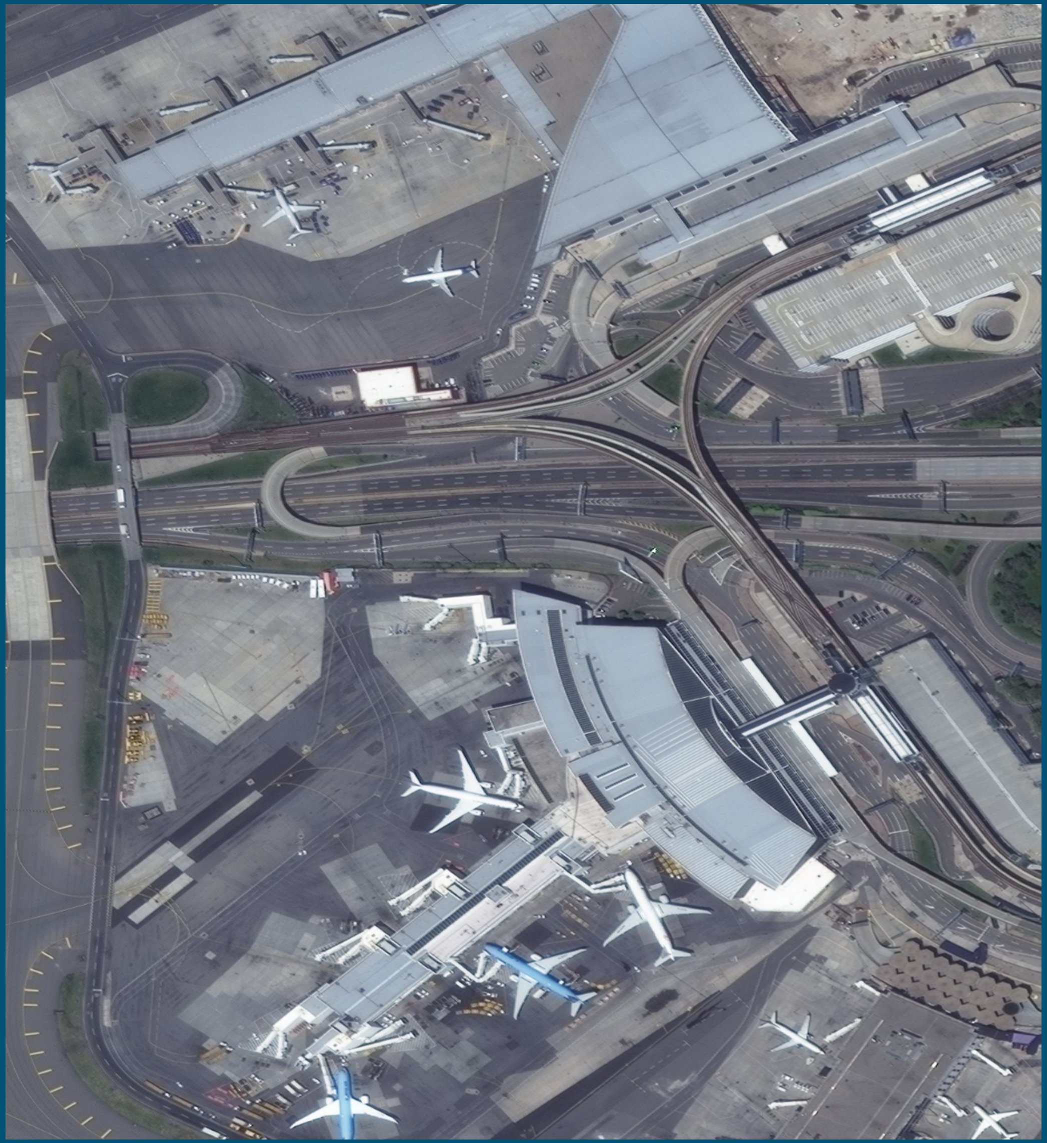
SAND2022-10717 C



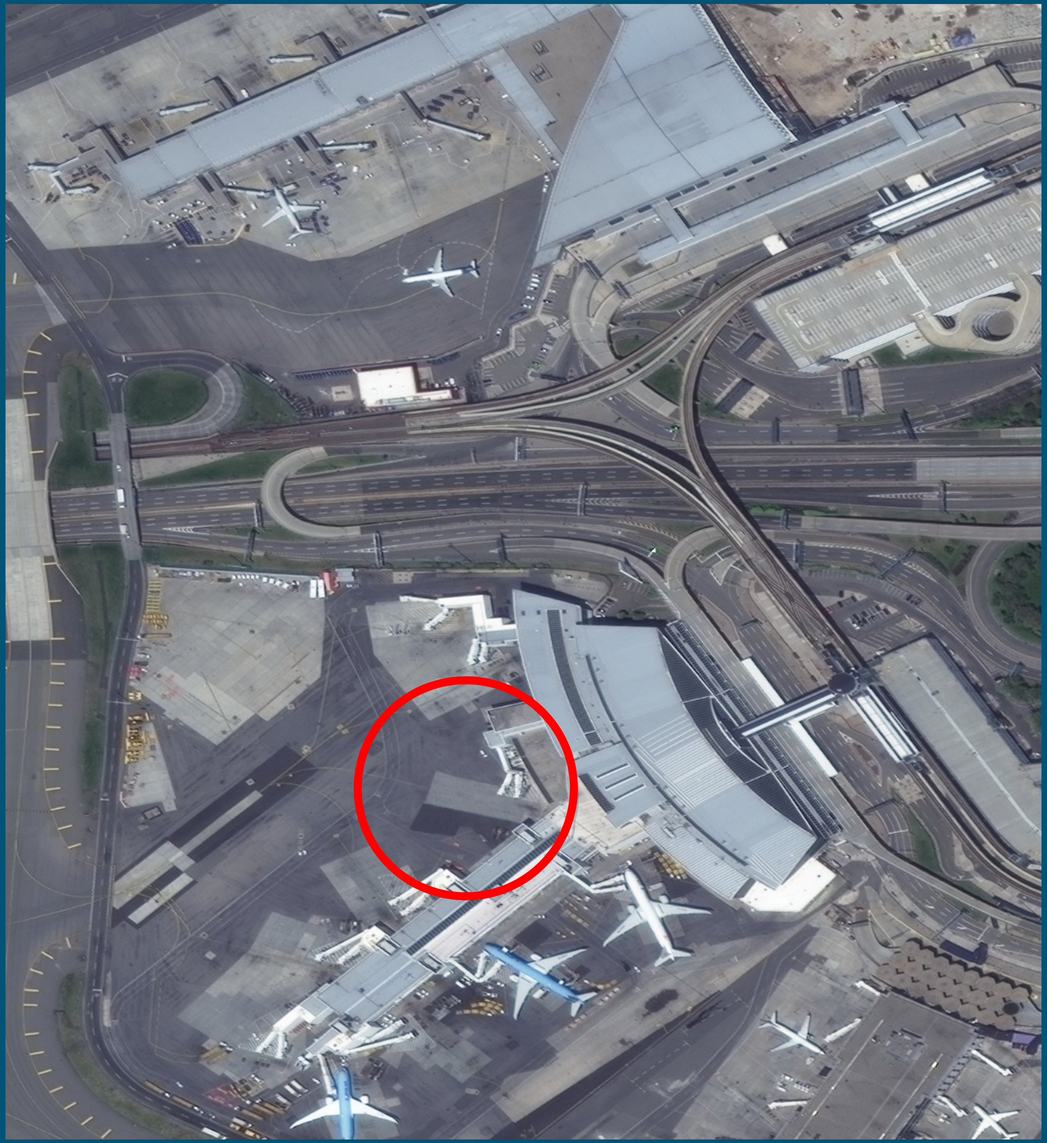
JFK Airport – May 10, 2020

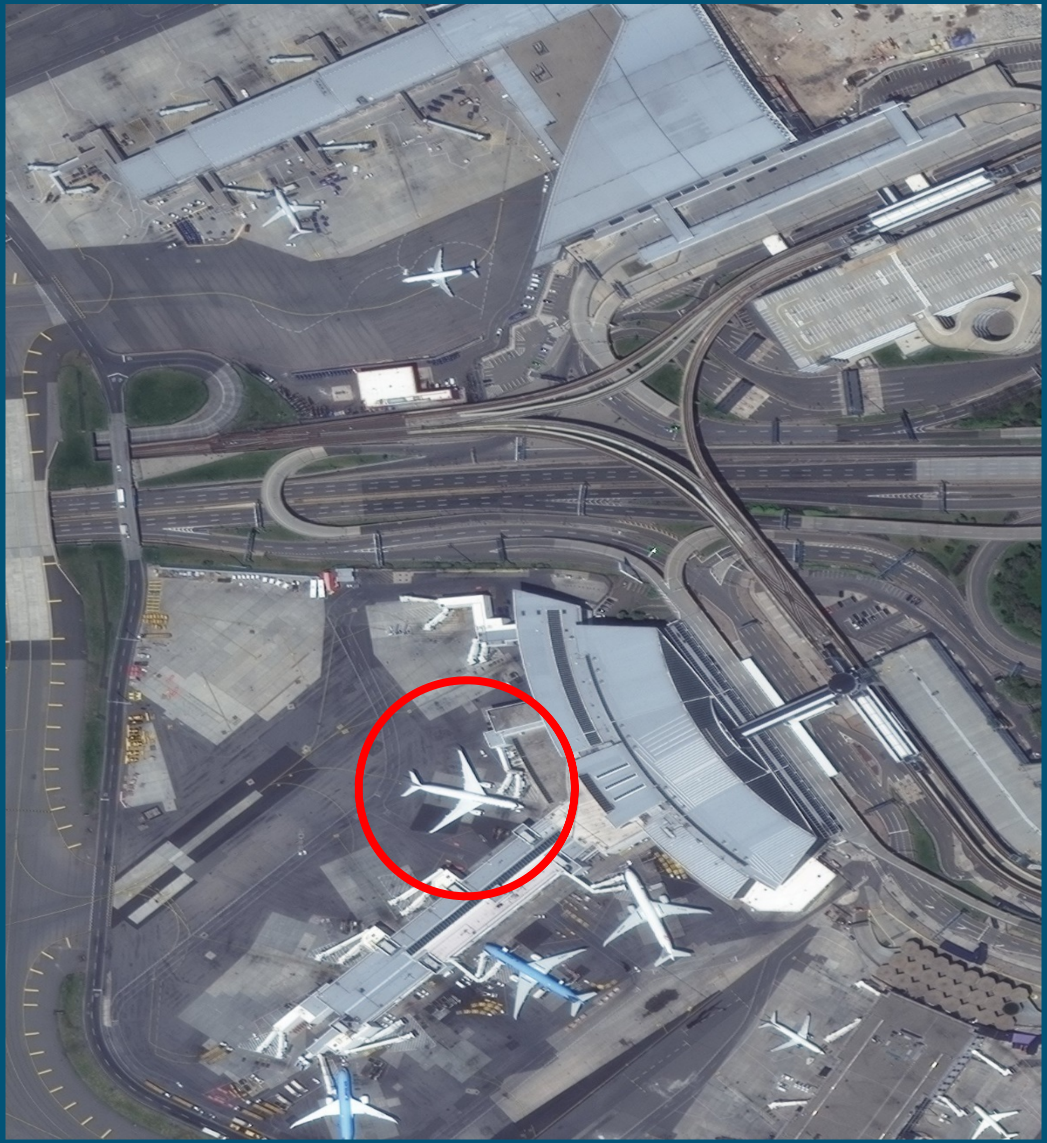
Spot the Difference





Which Image is the Original?





This is a presentation about assuring the authenticity of images created by third-party earth imaging sensors

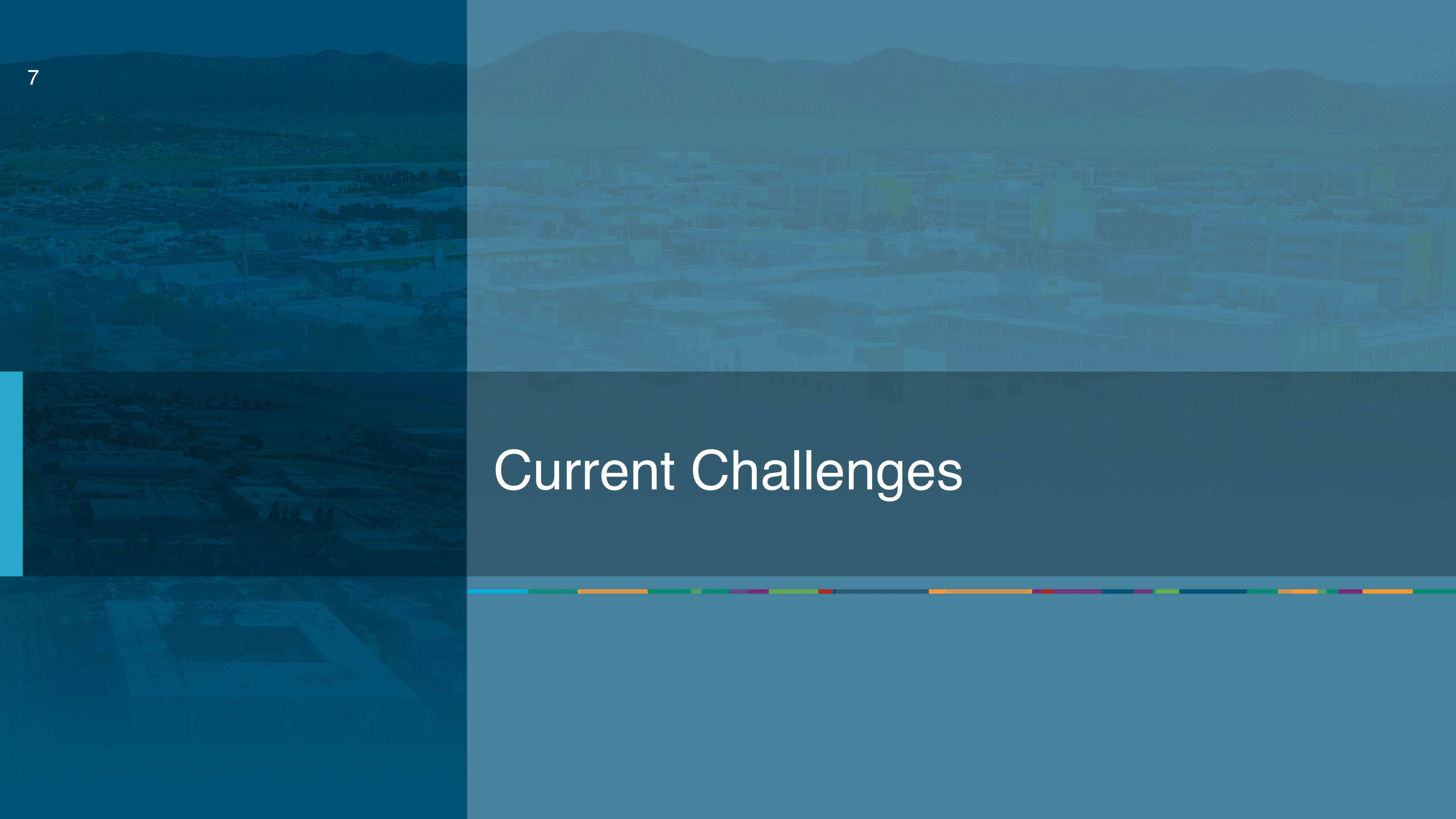
A third-party is one operated by a commercial company, government agency, or other external organization

Outline

Part 1: Current challenges

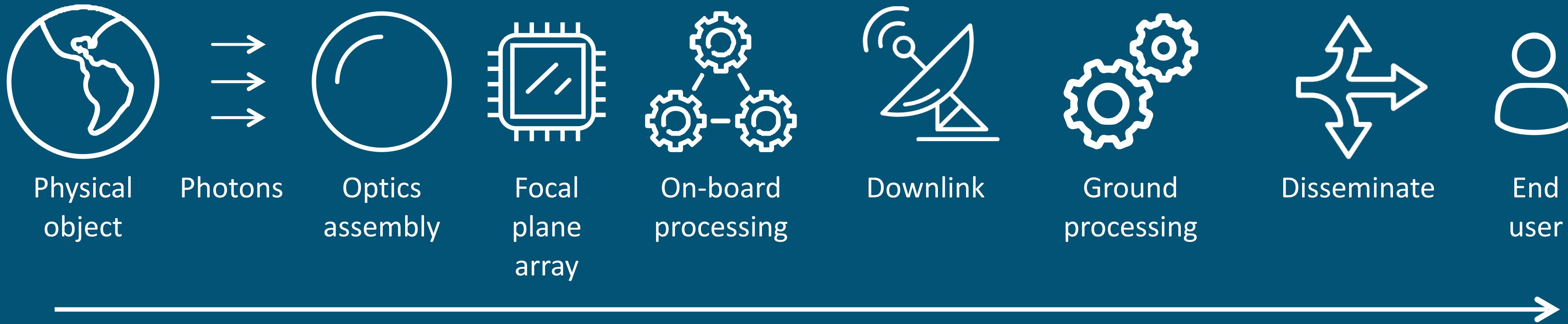
Part 2: Requirements for trust

Part 3: Architecture and verification



Current Challenges

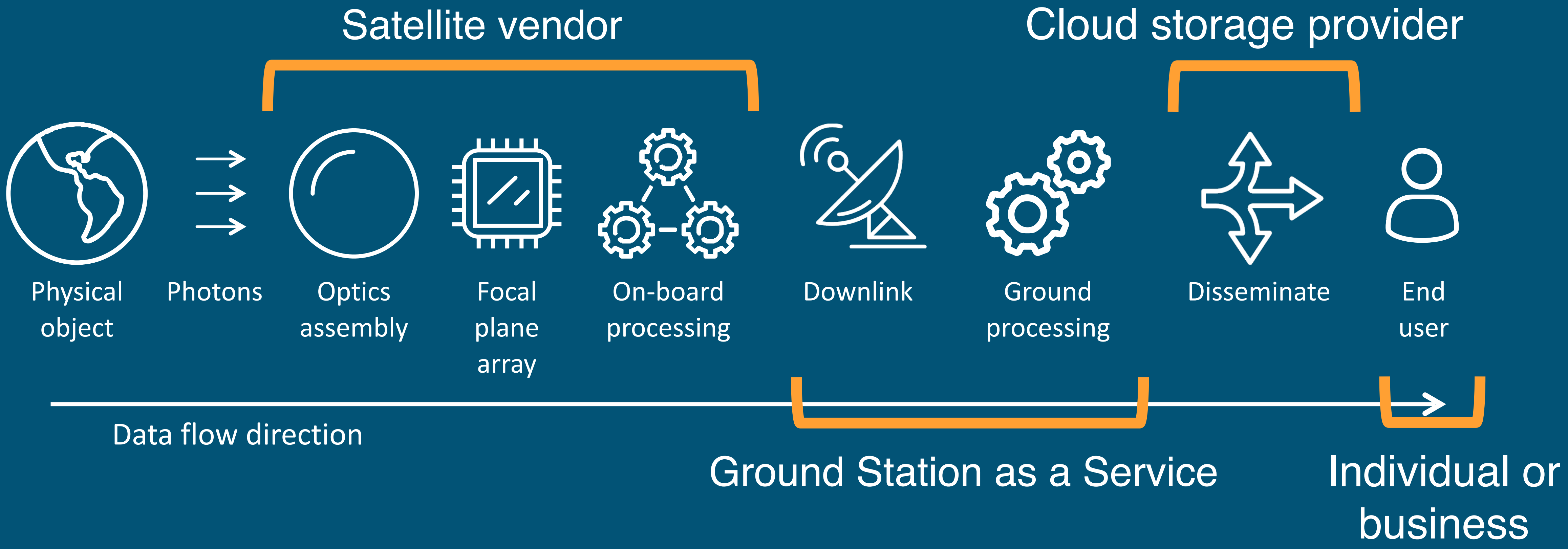
The Lineage of an Image



Data flow direction

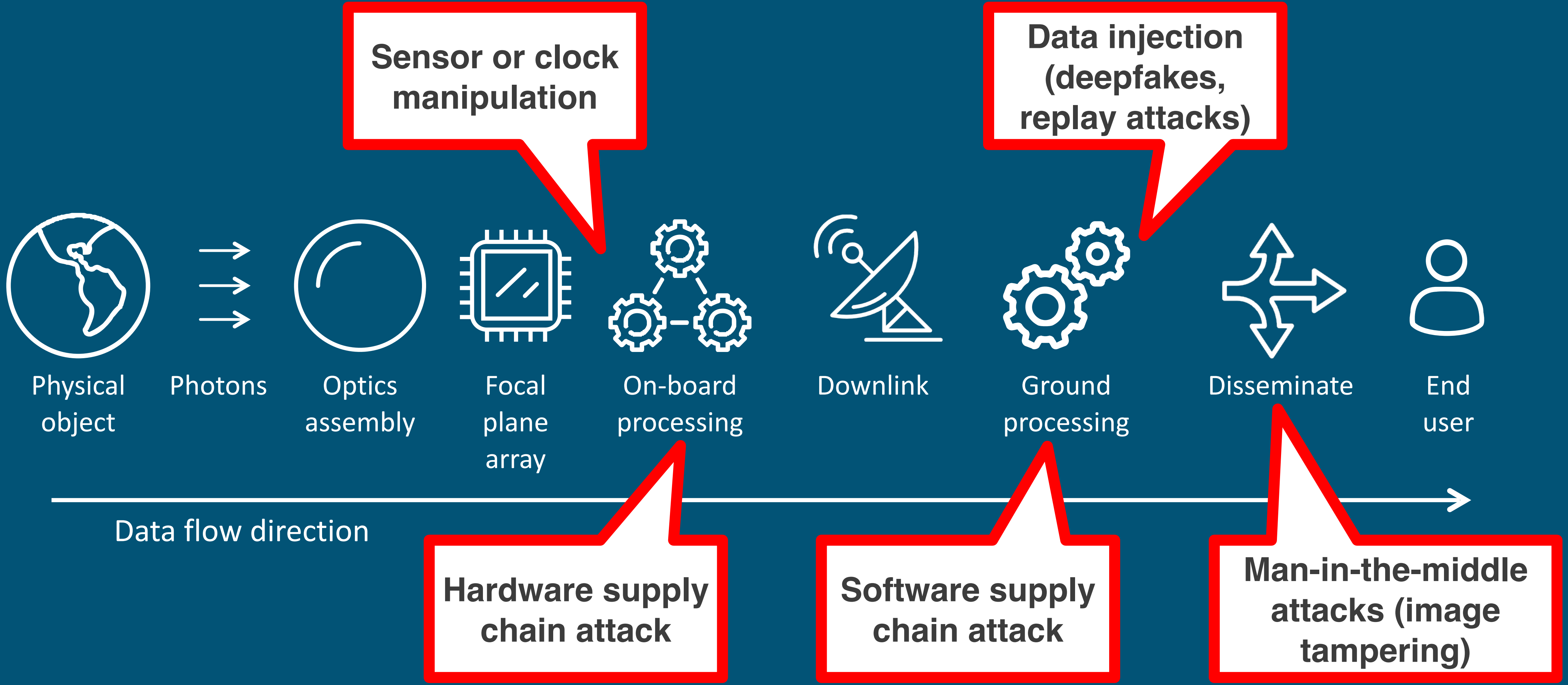
The data flows through several components and systems before reaching the end user

Challenge 1: Trust Segmentation



Trust is segmented as components and systems are built, owned, and operated by a different organizations

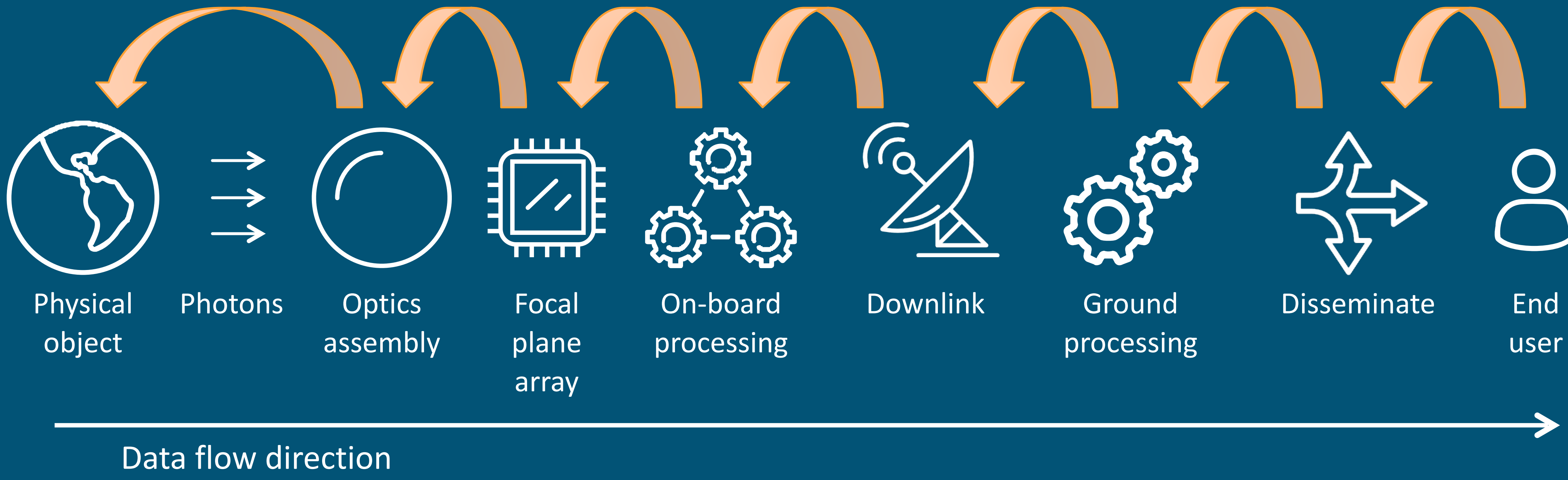
Challenge 2: Broad Attack Surface


Sensor or clock manipulation
Data injection (deepfakes, replay attacks)
Physical object
Photons
Optics assembly
Focal plane array
On-board processing
Downlink
Ground processing
Disseminate
End user
Data flow direction
Hardware supply chain attack
Software supply chain attack
Man-in-the-middle attacks (image tampering)

These systems and components could be vulnerable to various threats

Challenge 3: A Chain of Unguarded Trust

Each system simply trusts the system that sent the data



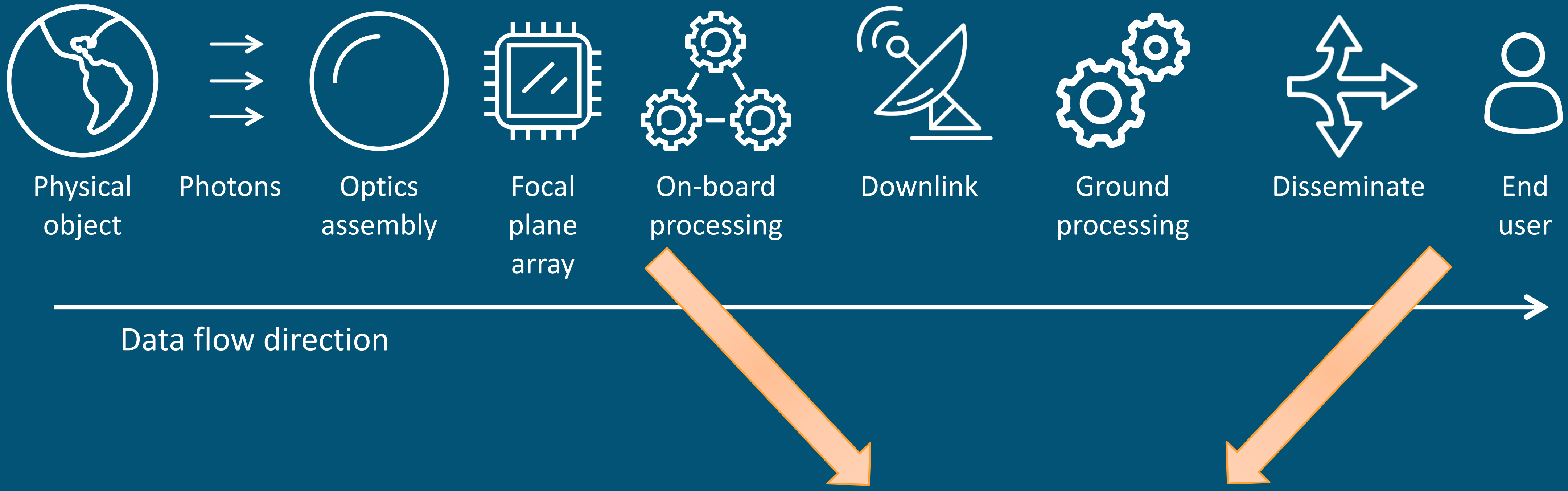
A game of telephone without end-of-round reconciliation!

Without end-to-end checks, nobody knows if the end product is authentic or not

Requirements For Trust

End-to-End Checking

Check authenticity by comparing end products against the image produced by the sensor



Physical object

Photons

Optics assembly

Focal plane array

On-board processing

Downlink

Ground processing

Disseminate

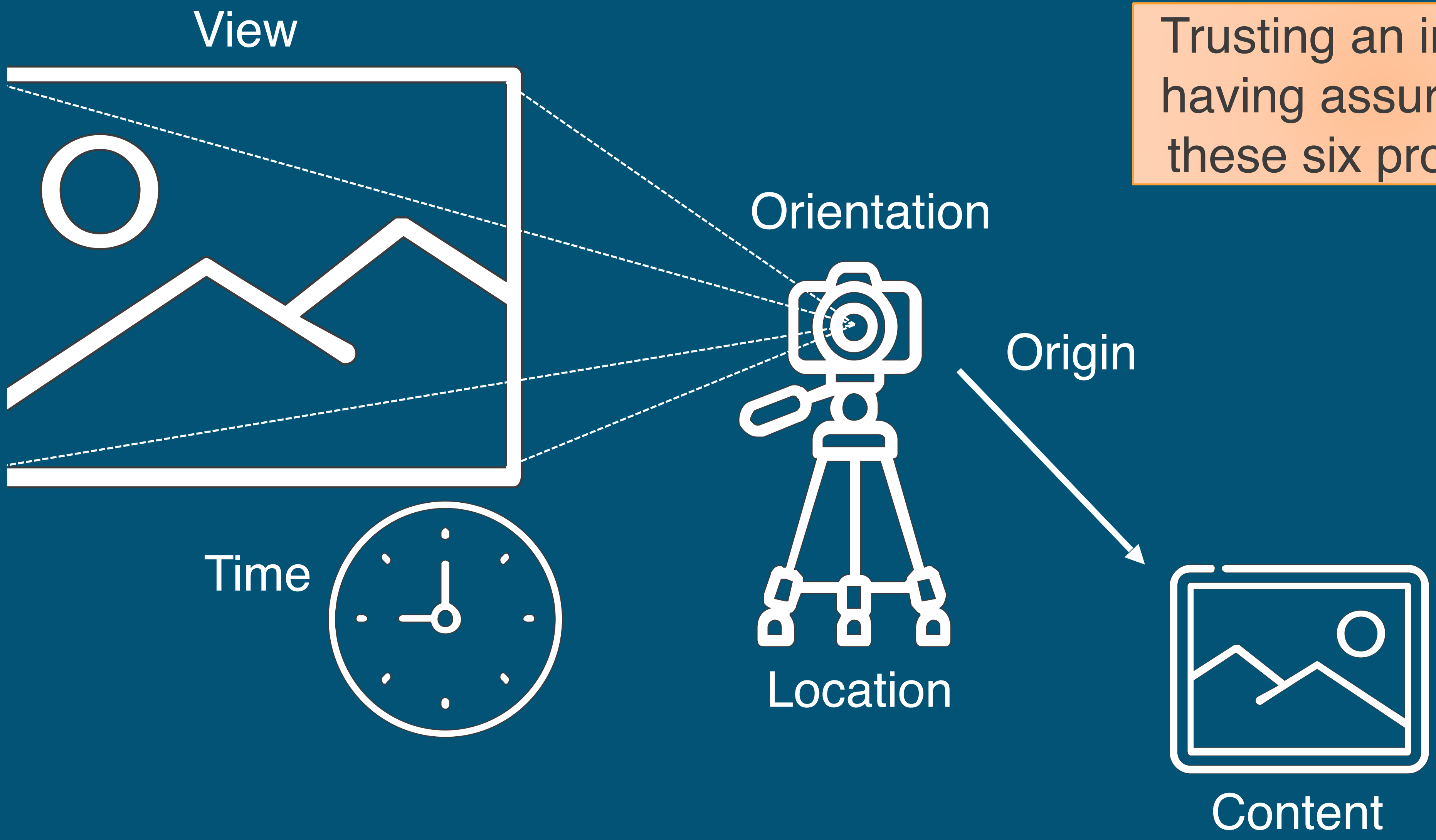
End user

Data flow direction

$$x = y$$

- Which properties must be checked?
- How is this done securely?

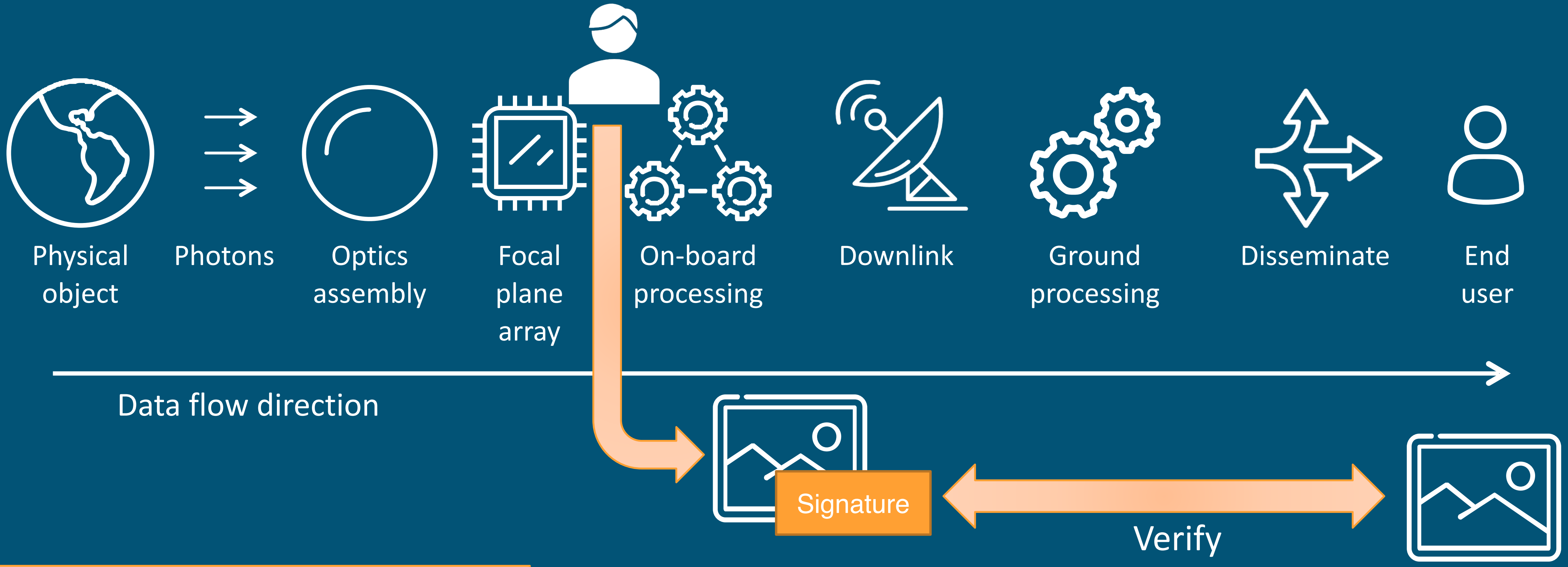
Requirements of Trust of Imagery



Trusting an image is having assurance of these six properties

Assurance of Original Image Properties

A digital “notary public” to sign off on the collection of an image



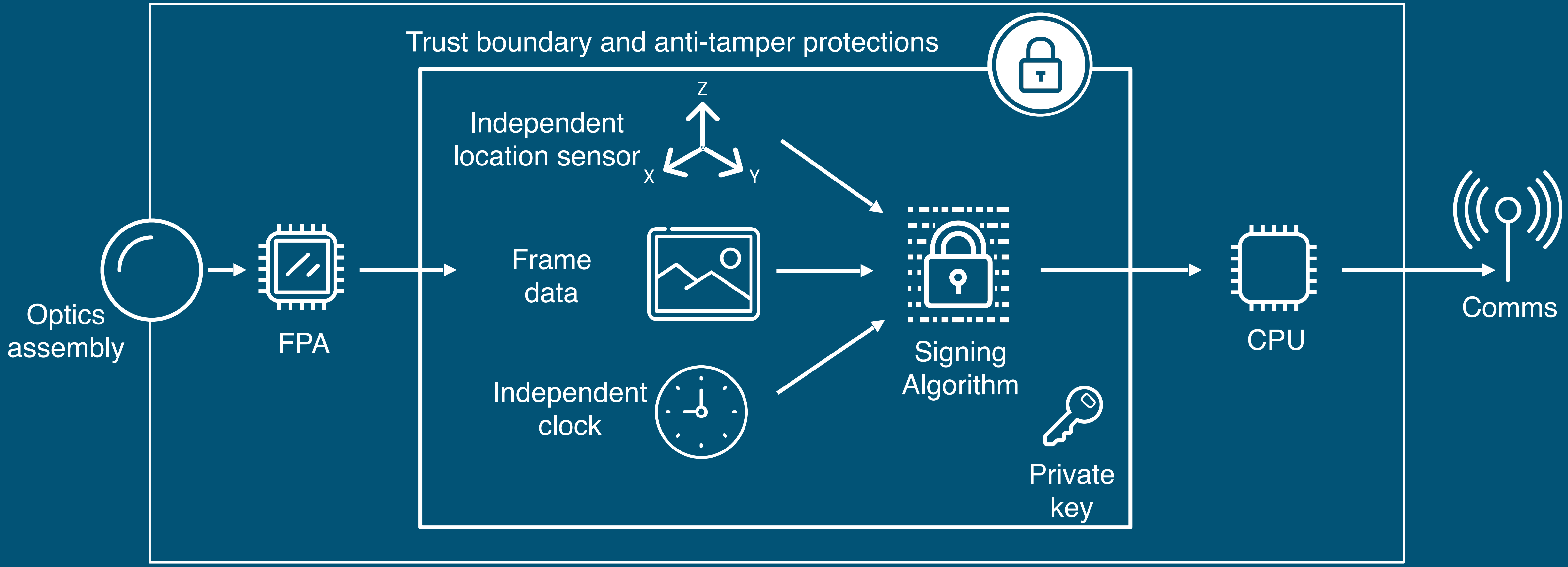
This independent verification bridges the trust gap between the vendor and the end user

A digital signature used as a proxy of the original data for comparison

Architecture and Verification

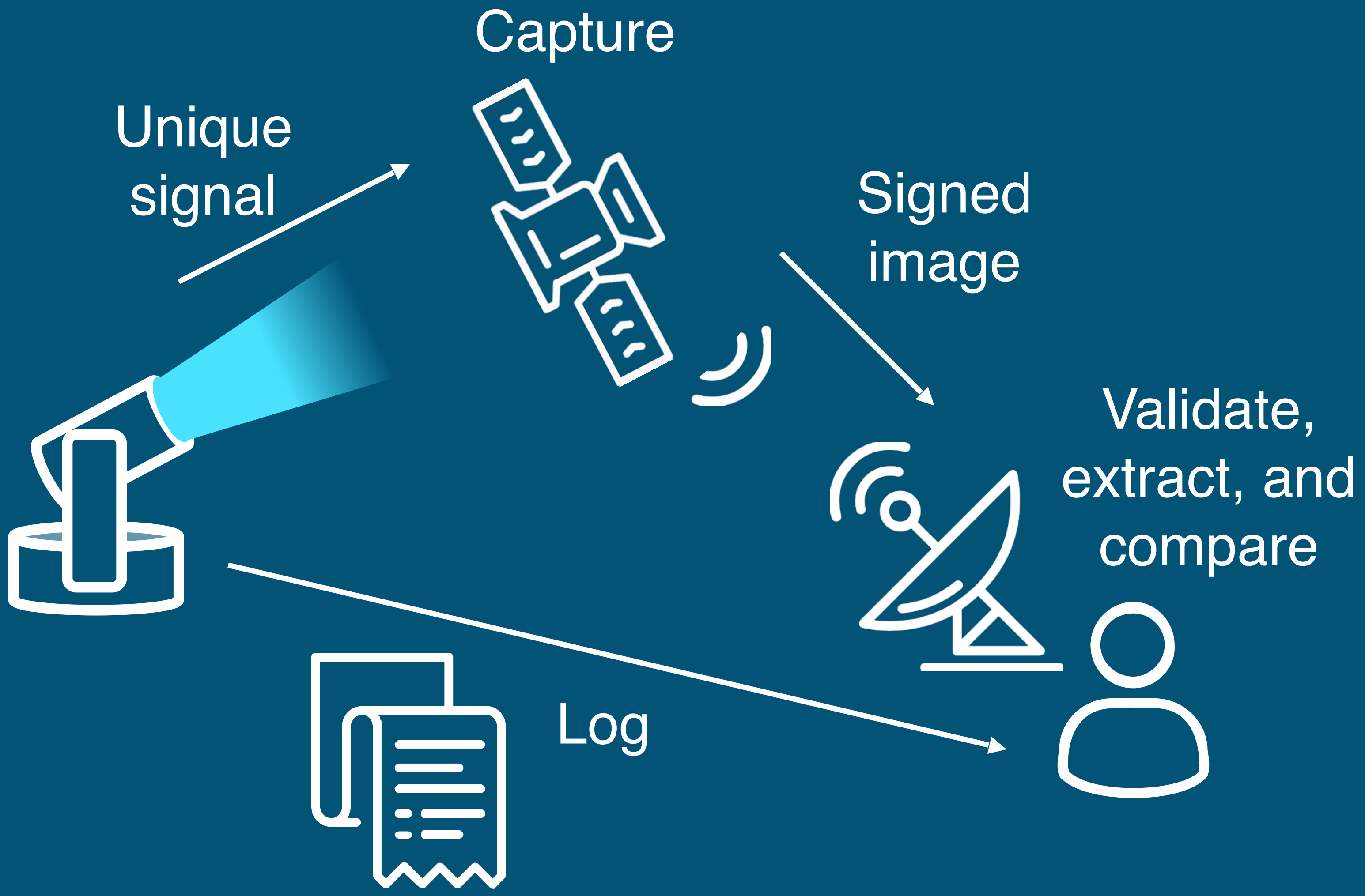
Our architecture and remote verification mechanisms are patent pending

Payload Architecture



Our architecture provides independent assurance of a satellite collection by signing the data, collect time, location information

Remote Verification: Emitter Test

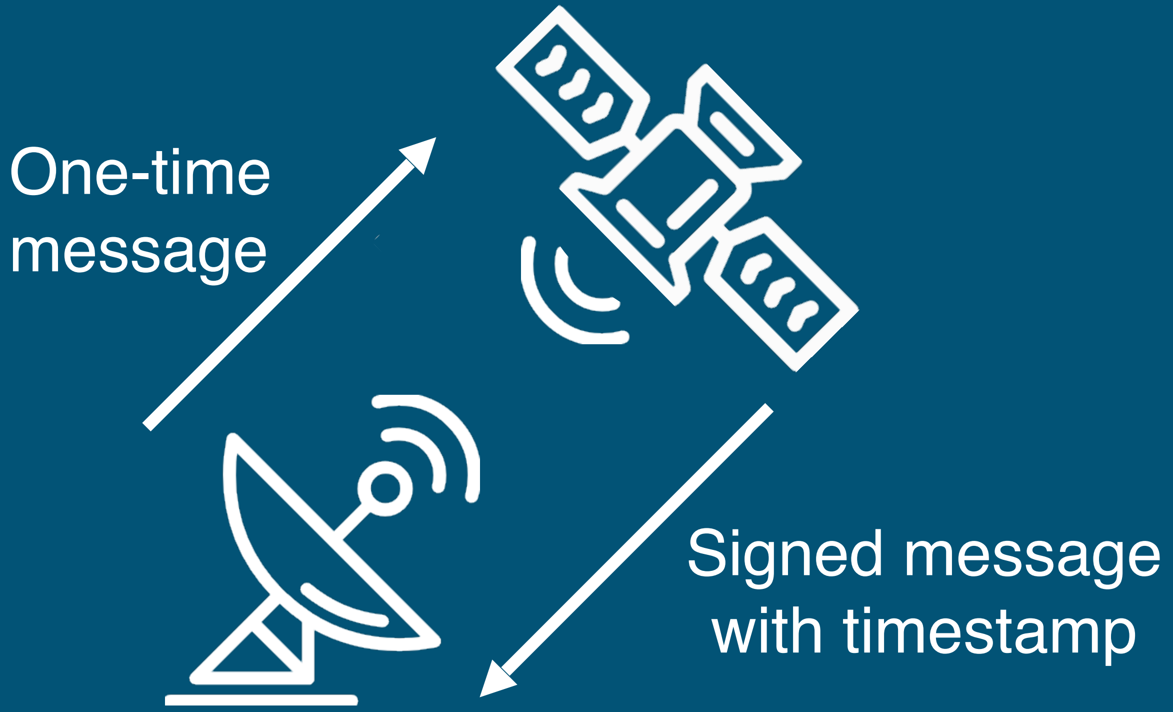


Trust requirements verified:

1. View
2. Orientation
3. Location
4. Origin
5. Content

This test exercises the full end-to-end data path: physical object to end user

Remote Verification: Challenge/Response Test



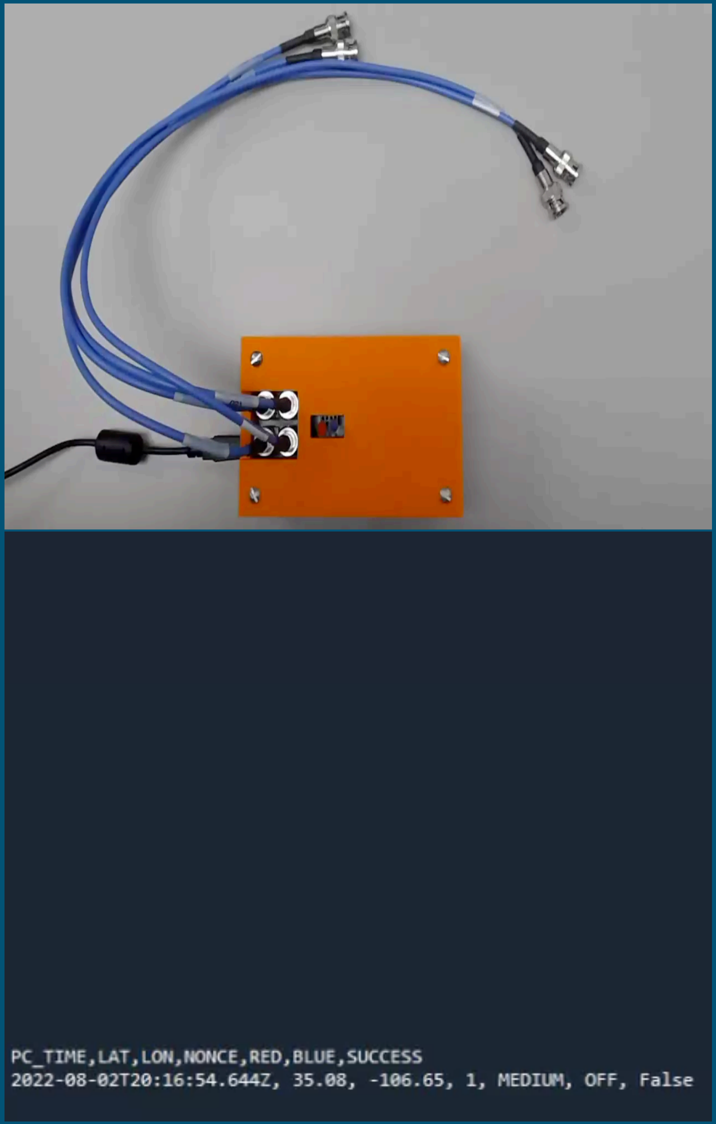
This test over RF commanding channels checks the trusted clock

Trust requirements verified:

1. Location
2. Origin
3. Time

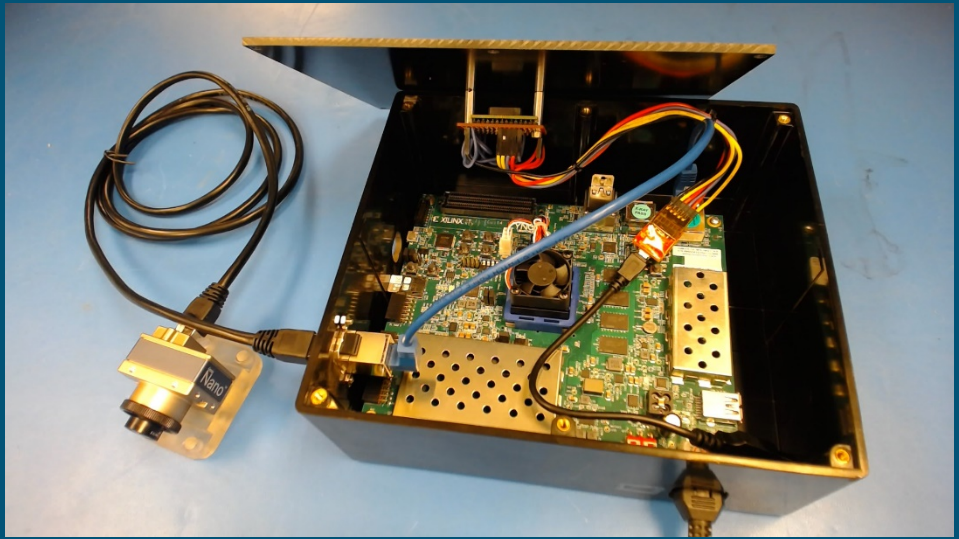
This bounded time test checks the trusted clock and confirms that the private signing key is on orbit

End-to-end Prototype (Lab Test)



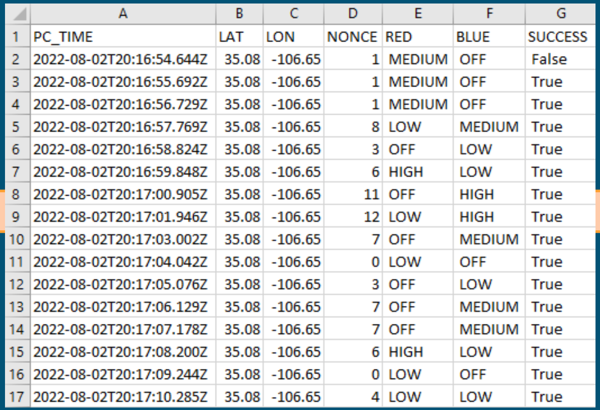
```
PC_TIME,LAT,LON,NONCE,RED,BLUE,SUCCESS
2022-08-02T20:16:54.644Z, 35.08, -106.65, 1, MEDIUM, OFF, False
```

Signal Generator



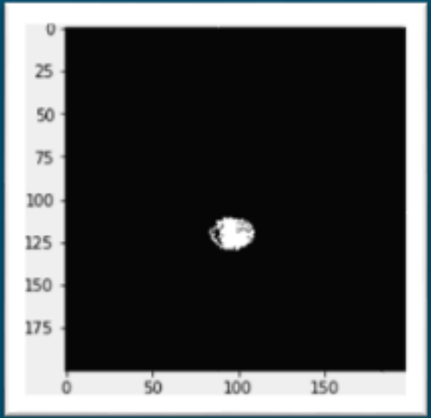
Prototype Trusted Hardware

End-user Verification



	A	B	C	D	E	F	G
1	PC_TIME	LAT	LON	NONCE	RED	BLUE	SUCCESS
2	2022-08-02T20:16:54.644Z	35.08	-106.65	1	MEDIUM	OFF	False
3	2022-08-02T20:16:55.692Z	35.08	-106.65	1	MEDIUM	OFF	True
4	2022-08-02T20:16:56.729Z	35.08	-106.65	1	MEDIUM	OFF	True
5	2022-08-02T20:16:57.769Z	35.08	-106.65	8	LOW	MEDIUM	True
6	2022-08-02T20:16:58.824Z	35.08	-106.65	3	OFF	LOW	True
7	2022-08-02T20:16:59.848Z	35.08	-106.65	6	HIGH	LOW	True
8	2022-08-02T20:17:00.905Z	35.08	-106.65	11	OFF	HIGH	True
9	2022-08-02T20:17:01.946Z	35.08	-106.65	12	LOW	HIGH	True
10	2022-08-02T20:17:03.002Z	35.08	-106.65	7	OFF	MEDIUM	True
11	2022-08-02T20:17:04.042Z	35.08	-106.65	0	LOW	OFF	True
12	2022-08-02T20:17:05.076Z	35.08	-106.65	3	OFF	LOW	True
13	2022-08-02T20:17:06.129Z	35.08	-106.65	7	OFF	MEDIUM	True
14	2022-08-02T20:17:07.178Z	35.08	-106.65	7	OFF	MEDIUM	True
15	2022-08-02T20:17:08.200Z	35.08	-106.65	6	HIGH	LOW	True
16	2022-08-02T20:17:09.244Z	35.08	-106.65	0	LOW	OFF	True
17	2022-08-02T20:17:10.285Z	35.08	-106.65	4	LOW	LOW	True

Signal Log



Signal Extractor

Pass/fail

Consider how you can integrate these principles of data authenticity into your satellite architectures

BE

AUTHENTIC

Thank you!

“The book is always better”

See our full paper for additional detail, including:

- Threats
- Architecture description
- Size, weight, and power constraints
- Post processing restrictions
- Inspection plans