RECEIVER INDEPENDENT IMPLEMENTATION OF THE GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OS-NMA)

ITSNT 2018: Navigation in Challenging Environment II

Xabier Zubizarreta, J. Rossouw van der Merwe, Ivana Lukčin, Alexander Rügamer, Wolfgang Felber

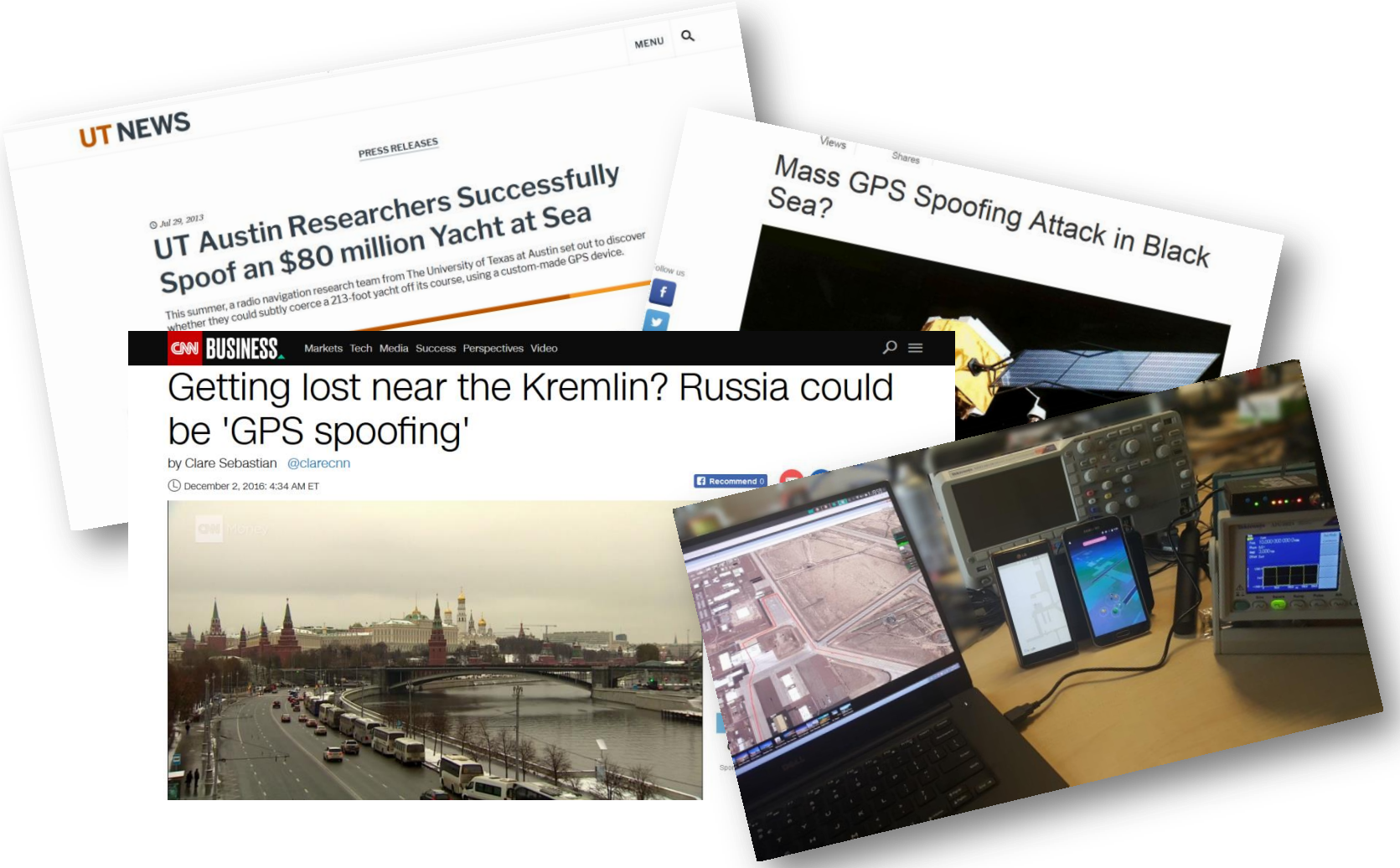
xabier.zubizarreta@iis.fraunhofer.de
Fraunhofer IIS, Nuremberg

European Global Navigation Satellite Systems Agency

HORIZON 2020

Fraunhofer IIS

The threat of spoofing



European Global Navigation Satellite Systems Agency

HORIZON 2020

Fraunhofer IIS

Need of protection

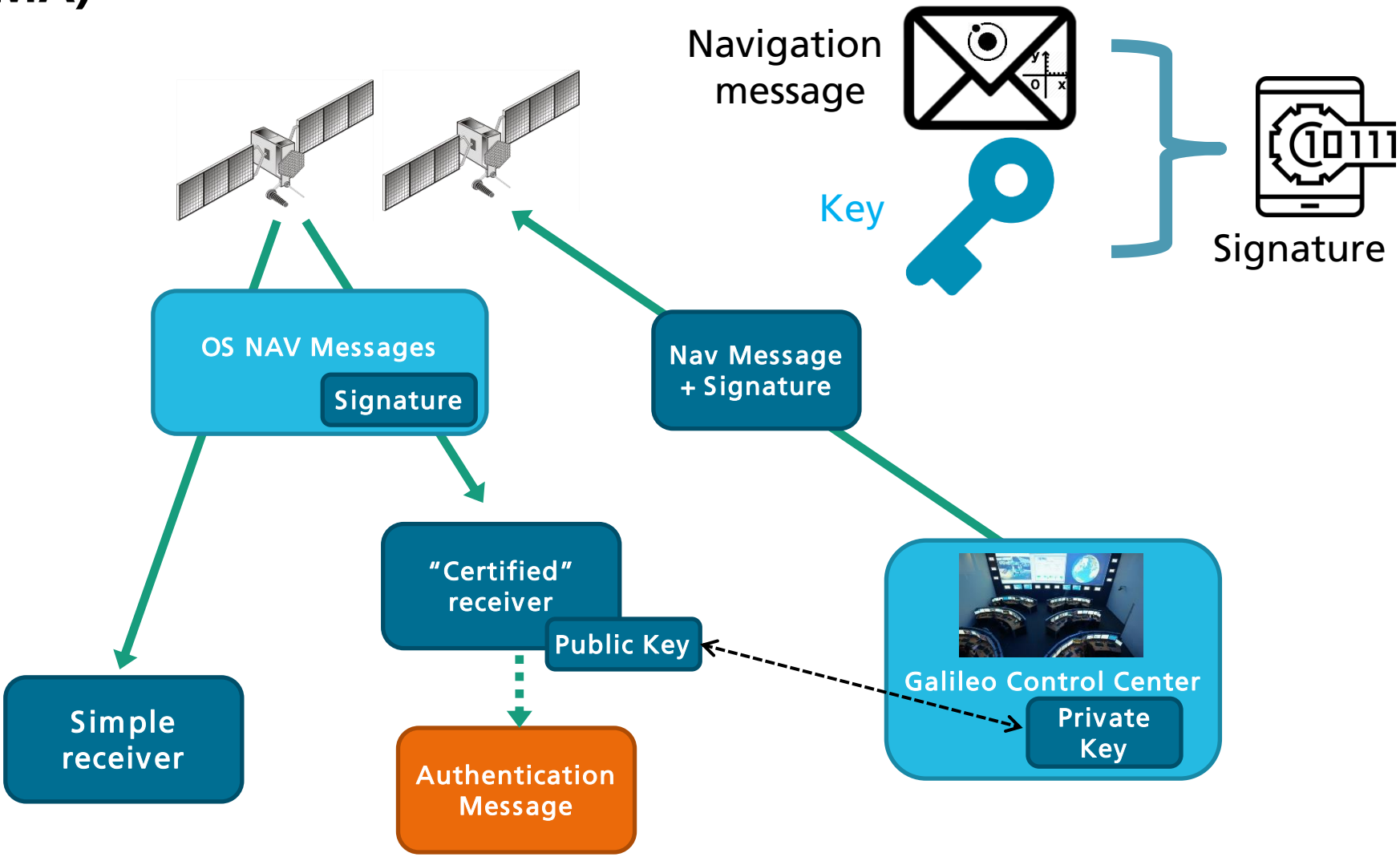
- Authentication at **signal level** (e.g. Galileo Public Regulated Service)

- Authentication at **message level**

AGENDA

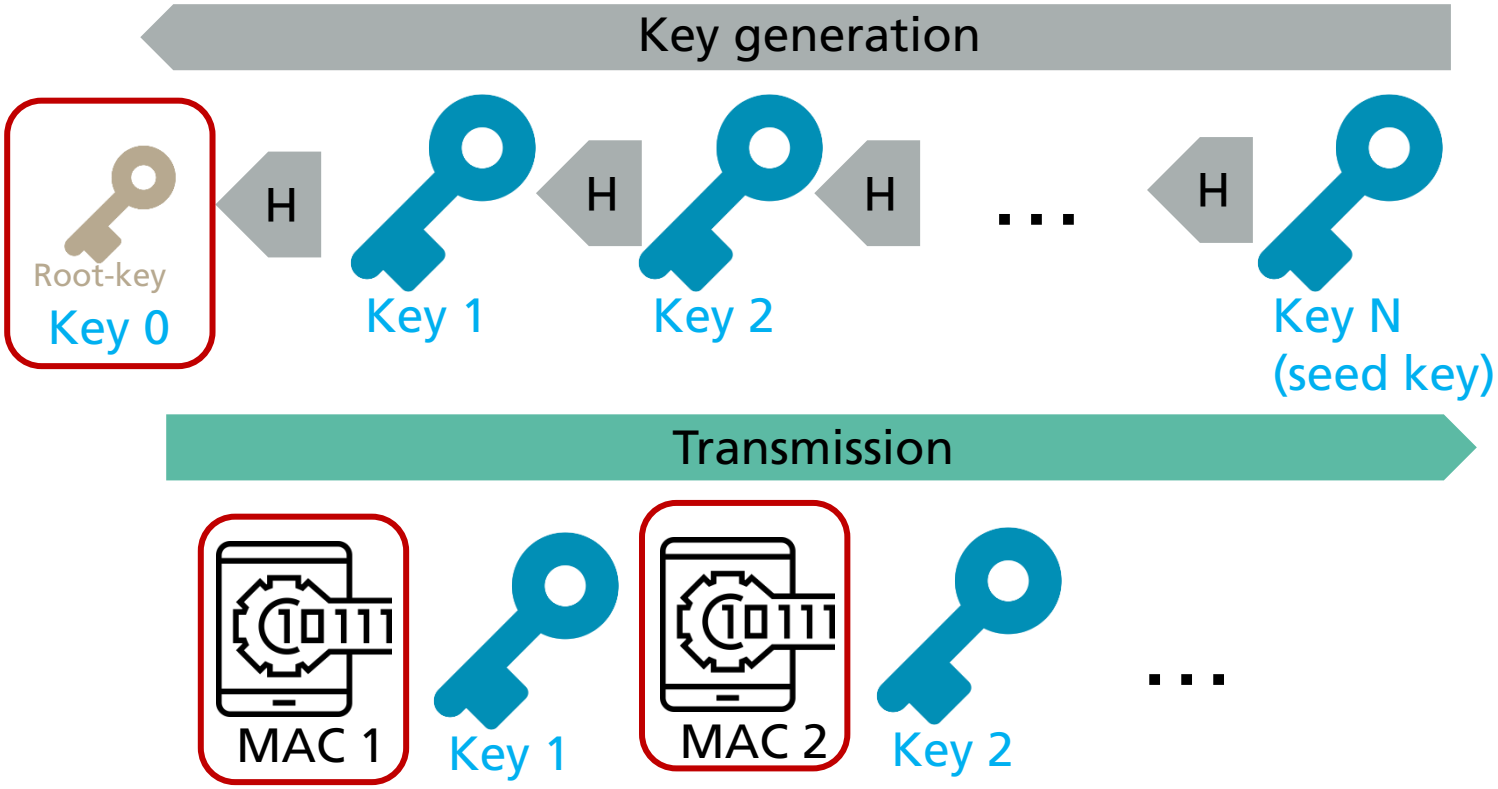
- Introduction to OS-NMA
- Implementation
- Advantages, disadvantages, constraints, and dangers

Open Service Navigation Message Authentication (OS-NMA)



OS-NMA: A brief description

- Timed Efficient Stream Loss-tolerant Authentication (**TESLA**)
- 1) Root key verifies all keys
- 2) Each key verify the **previous** Message Authentication Code (**MAC**)

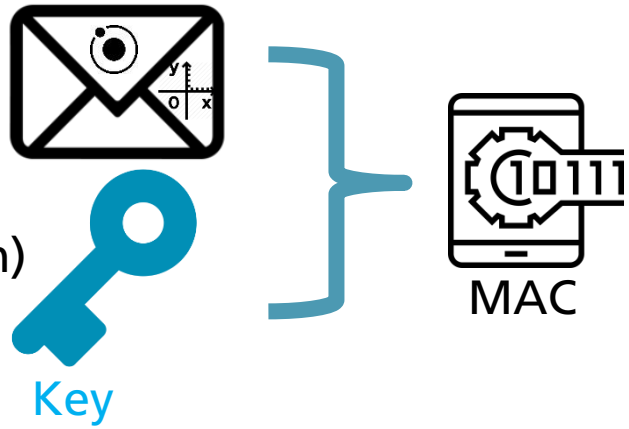


OS-NMA: A brief description

- Assymetrical cryptography (slow, done only once)
  - Elliptic Curve Digital Signature Algorithm (ECDSA) → 448-1043 bits
- Symmetrical cryptography (fast, done for key / MAC generation)
  - Hash-based message authentication code (HMAC) → 256 bits → Truncate

ECDSA (Root-key authentication)

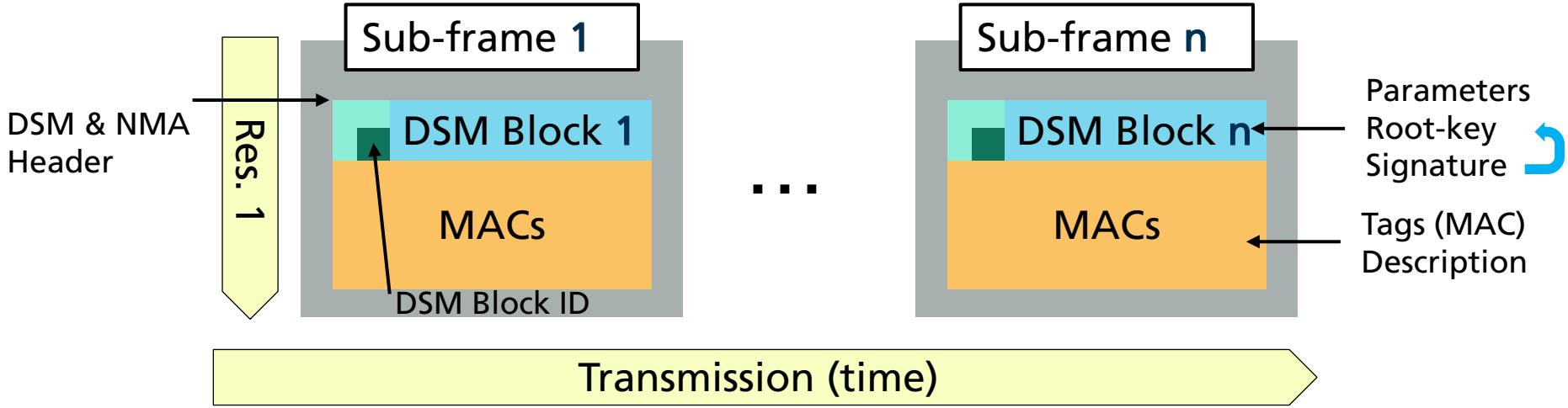
HMAC (Nav. msg. authentication)



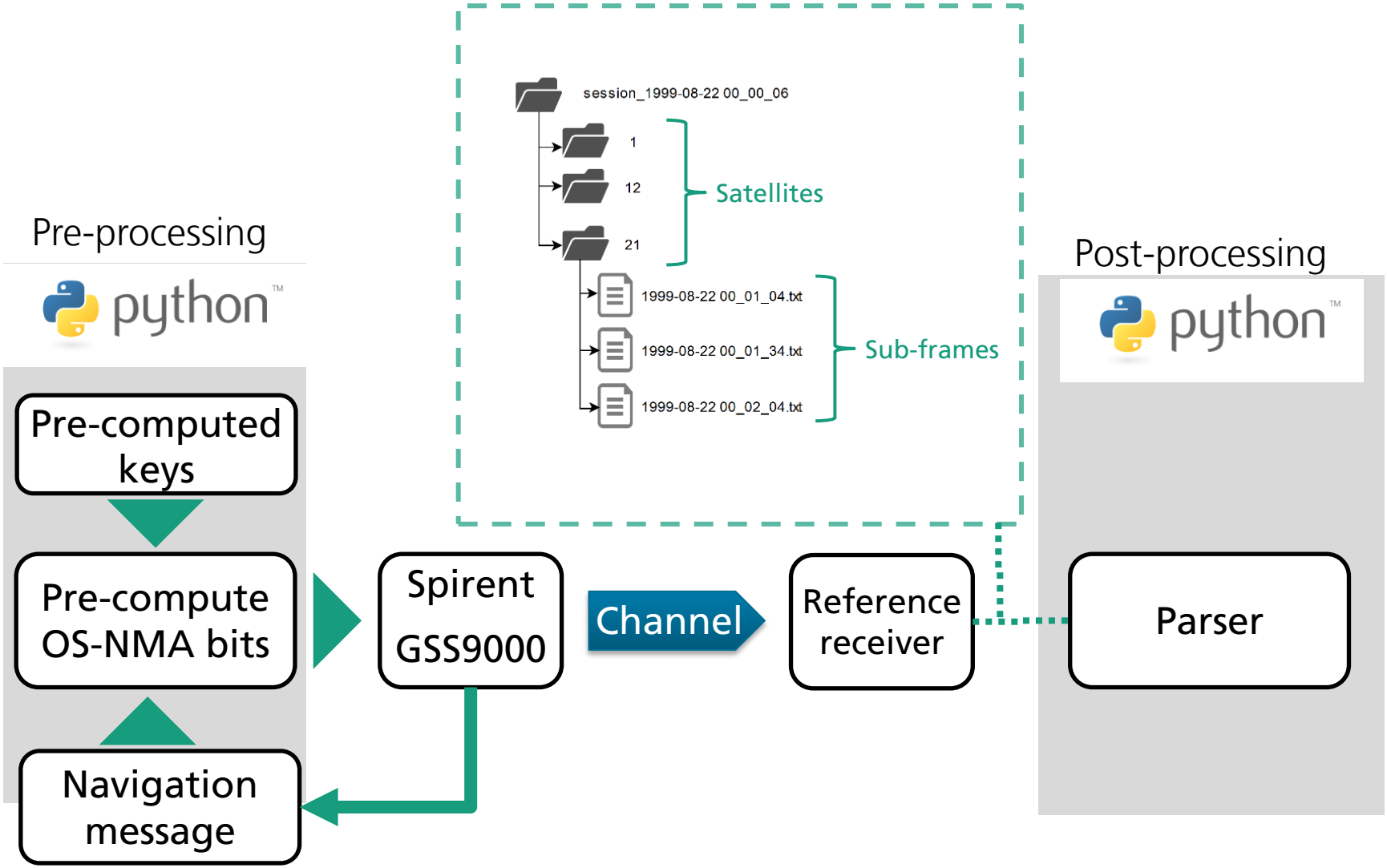
OS-NMA: A brief description

	E1-B									
	Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRC_j	Reserved 2	Tail	Total (bits)
even	1	1	16	40	22	2	24	8	6	120
	Even/odd=0	Page Type	Data k (1/2)						Tail	Total (bits)
odd	1	1	112						6	120

- I/NAV: 40 bits every 2 seconds
- Subframe : 600 bits (40 bits x 15 pages)
- Header & Root-key (HKROOT): 120 bits (!)
  - Header
  - Digital Signature Message (DSM) Block
  - 6 - 16 subframes (3 to 8 minutes)
- MAC section : 480 bits
  - Contains the signatures



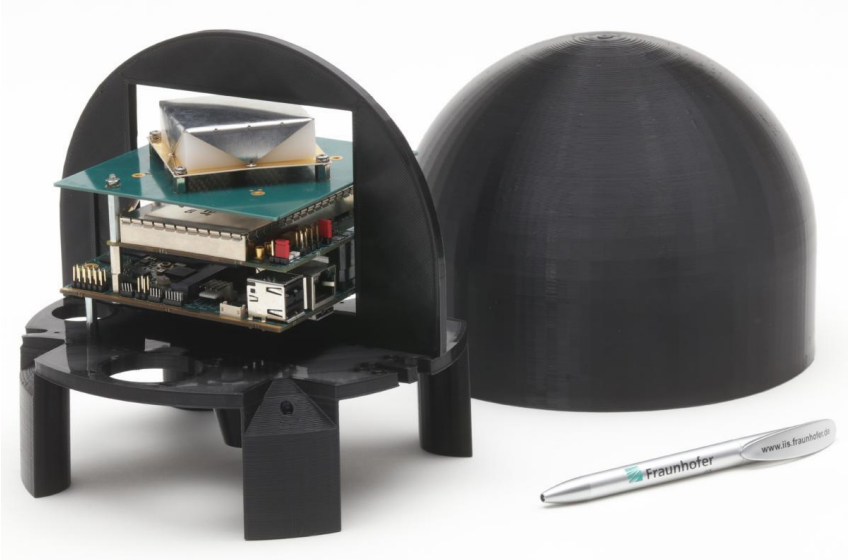
Implementation set-up



Receiver Independent

- Raw navigation message bits available:

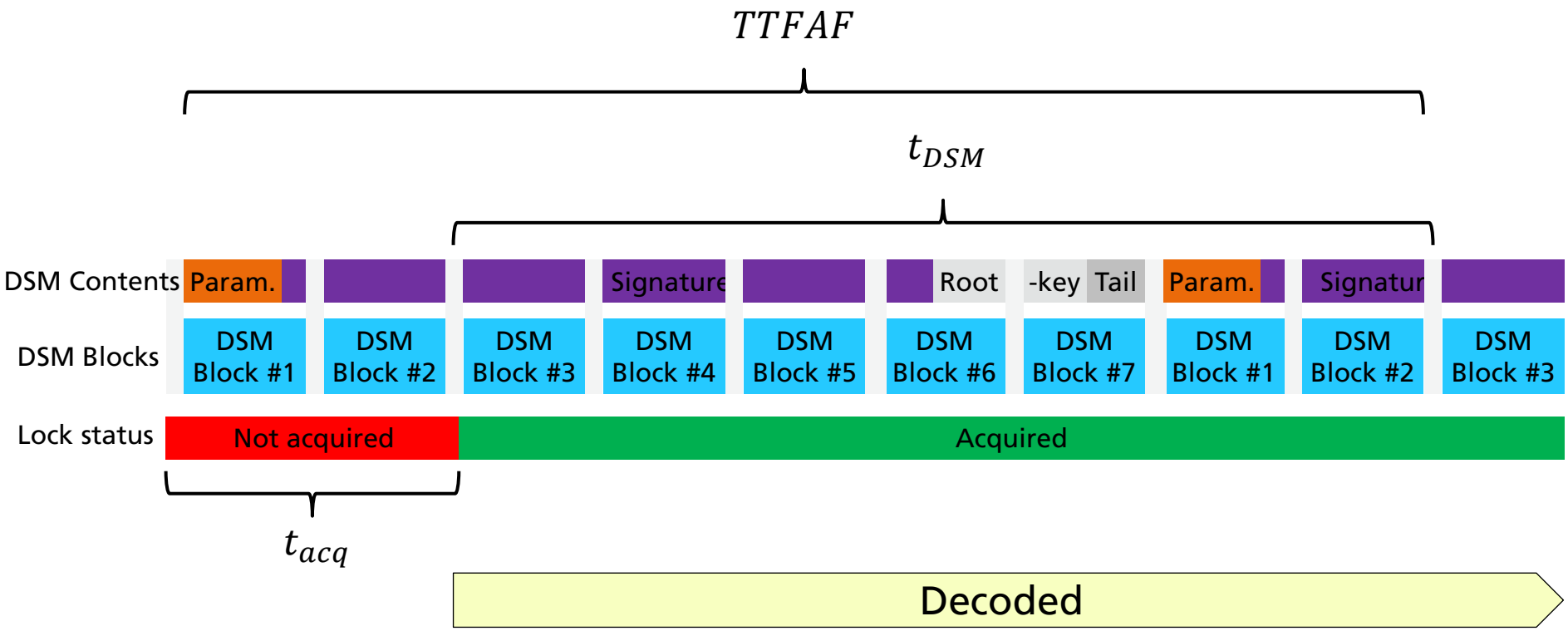
Manufacturer	Receiver	Raw bits
Septentrio	PolaRx5	Accessible as GalRawINAV
u-blox	M8T	Accessible in UBX-RXM-SFRBX
Fraunhofer IIS	GOOSE	Custom direct write to file
Android	Selected smartphones	Accessible in GNSS Raw Data*



*From API 24 onwards

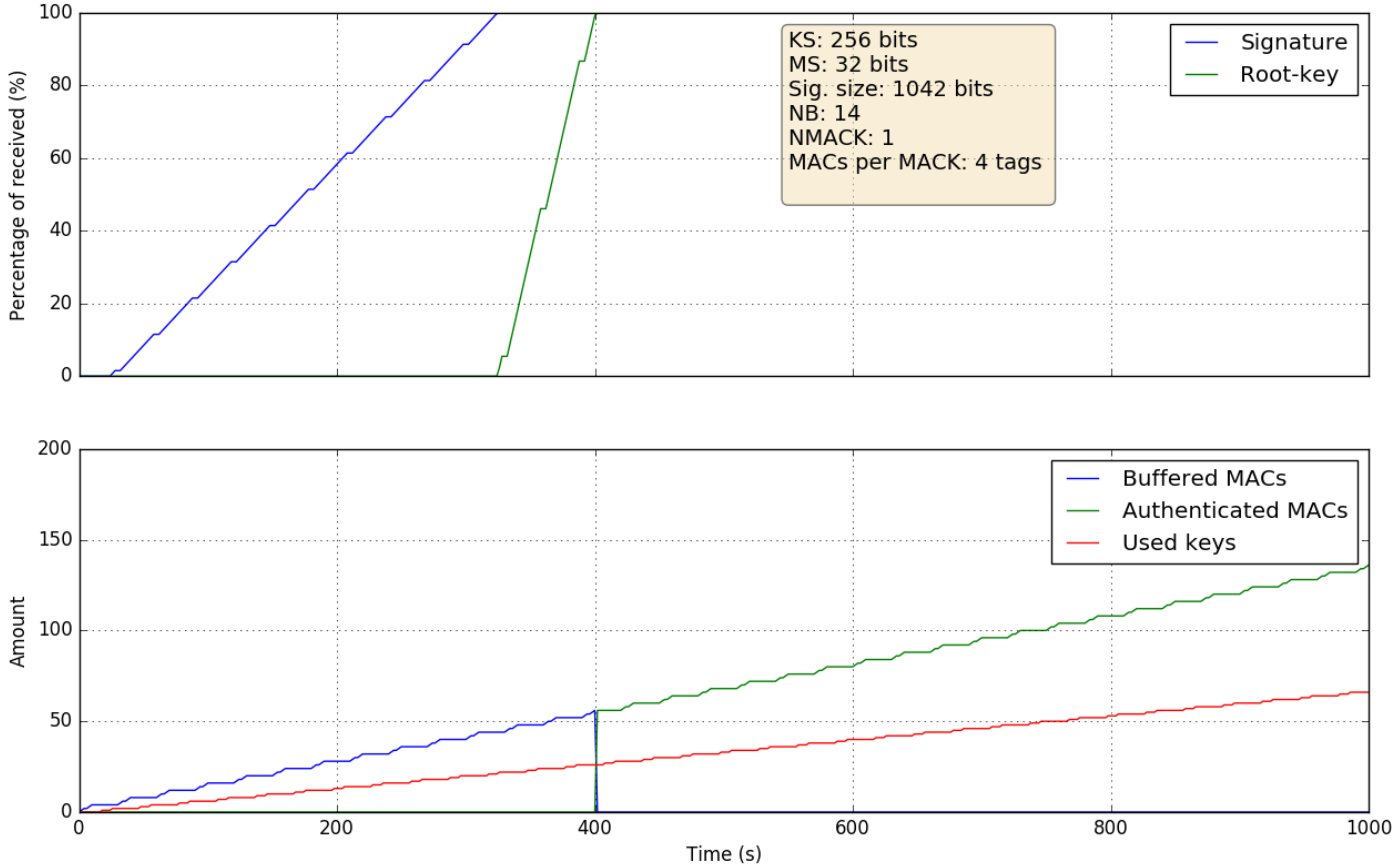
Constraints: Time

- Time to First Authenticated Fix (TTFAF)
- From cold-start



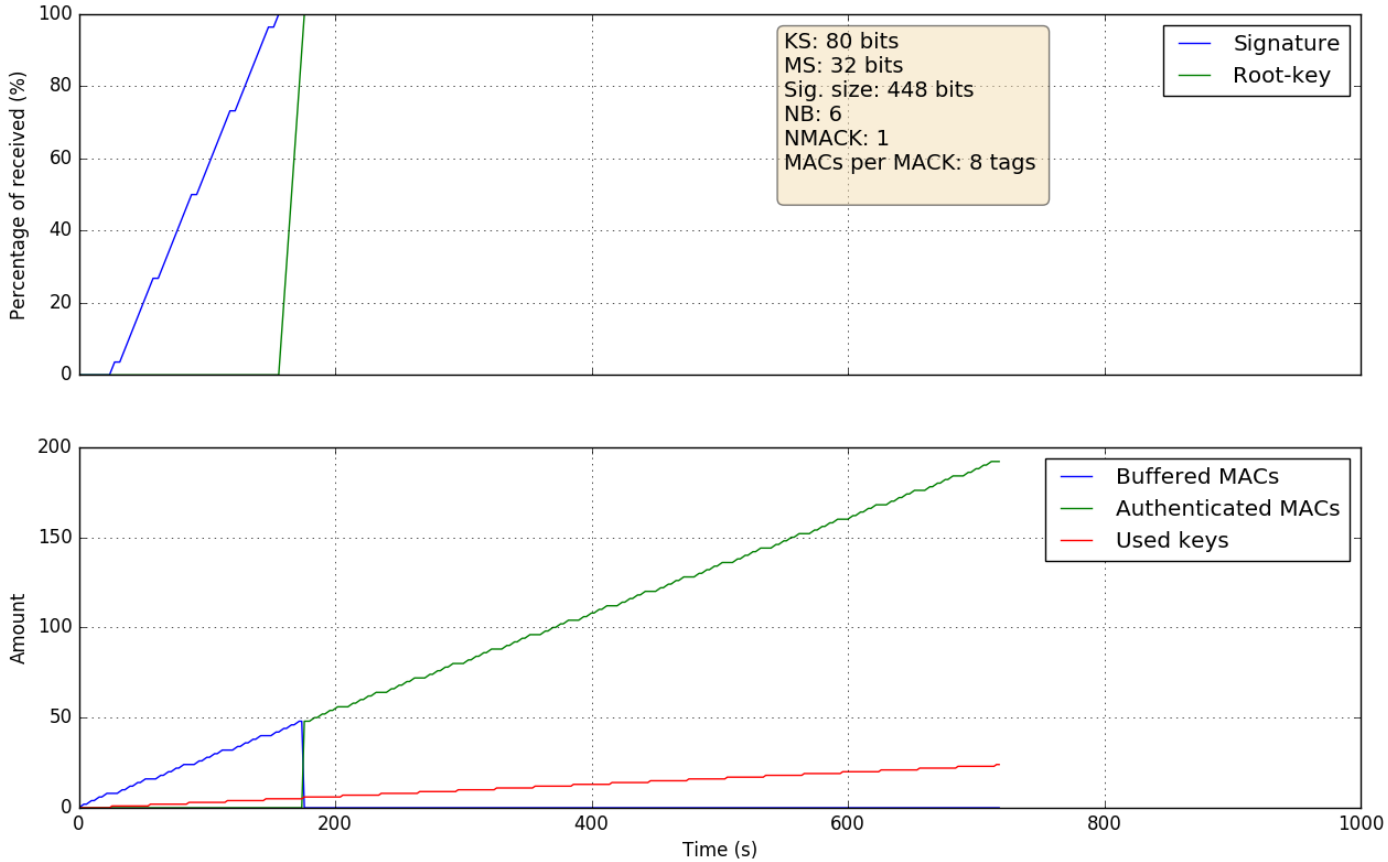
Constraints: Time

- Slowest case ca. 420 seconds



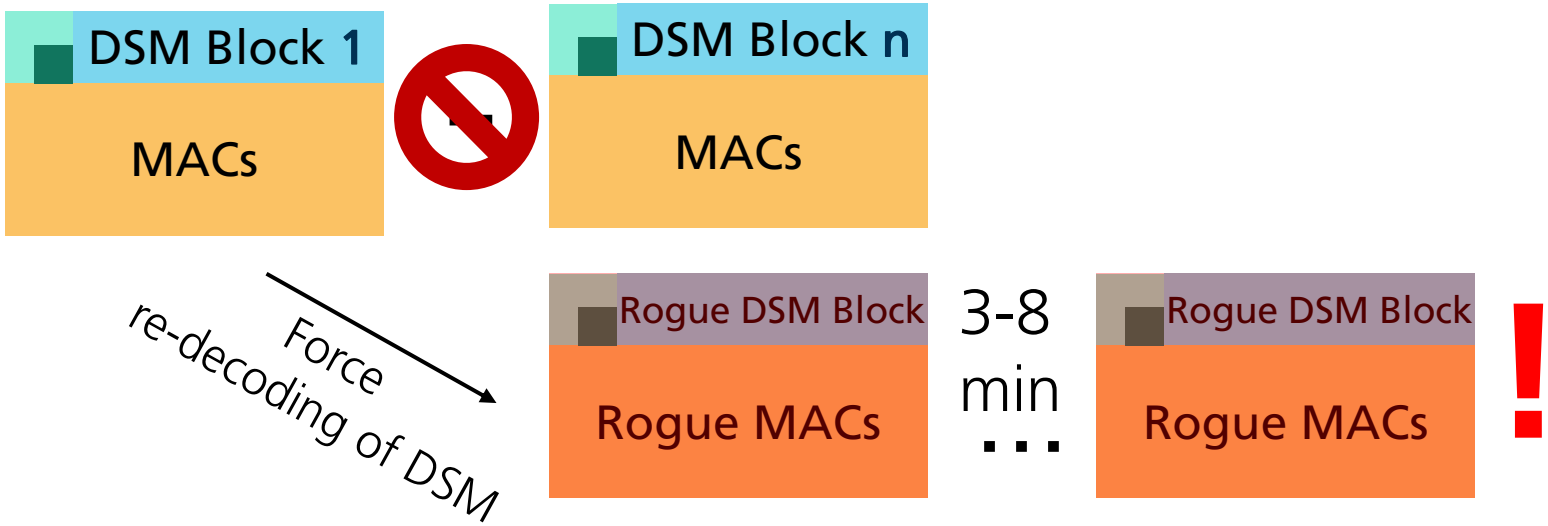
Constraints: Time

- Fastest case 180 seconds (from cold start)

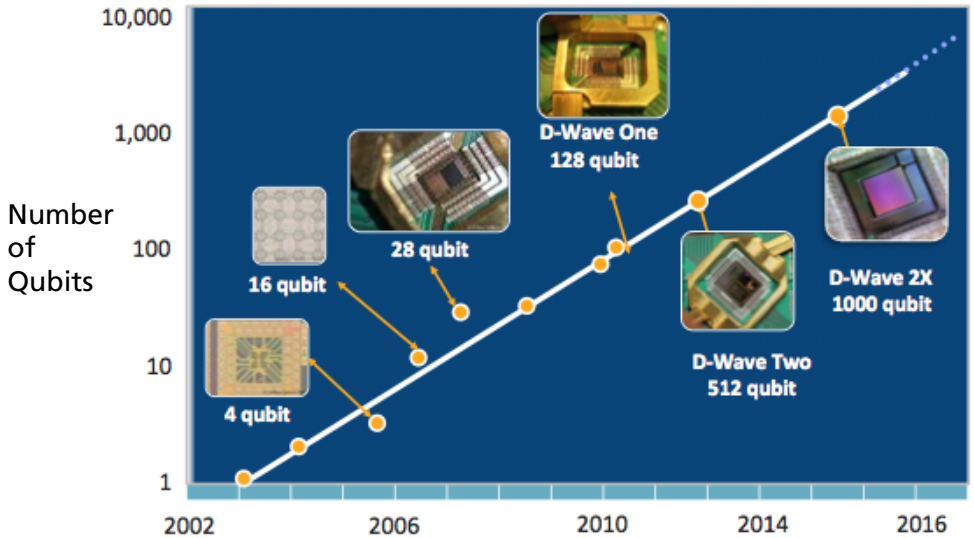


Constraints: Time to first alert

- Deny the signal and force re-decoding
- Avoided pre-trusting keys



Constraits: Security of algorithms



- Symmetric cryptography → Hashing is quantum safe
- Asymmetric cryptography → ECDSA is **not** quantum safe!

Use-cases

Source: ©KRoock74

Source: ©Vladislav Bezrukov

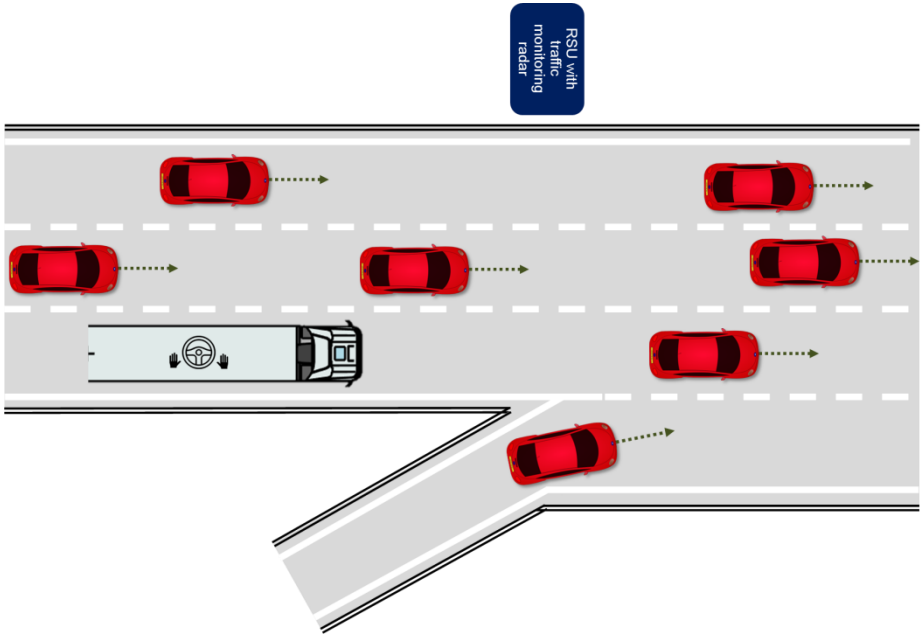
European Global Navigation Satellite Systems Agency

HORIZON 2020

Fraunhofer IIS

Use-cases: Project PRoPART

- The main objective of the PRoPART is to **develop and demonstrate a high availability positioning solution for connected automated driving applications.**
- enhance an existing RTK (Real Time Kinematic) software solution by **exploiting the distinguished features of Galileo signals**



Conclusions: Why / why not OS-NMA?

Open Service

Secure nav. msg.

Low impact on TTF(A)F*

Firmware update only

Ground segment

Long time to alarm

Replay attacks

Spreading authentication

THANK YOU!

Questions?

Contact: xabier.zubizarreta@iis.fraunhofer.de

The work for this paper has been conducted under the PRoPART project, which has received funding from the European GNSS Agency under the European Union's Horizon 2020 research and innovation program under grant agreement No 776307.

European Global Navigation Satellite Systems Agency

HORIZON 2020

Fraunhofer IIS