State of the art in signal authentication schemes for open satellite navigation services

Oscar Pozzobon

Qascom

Qascom
Trust is Nice, Control is Better.

Where are we?

- GPS no civilian authentication. Egnos, no authentication, Galileo CS might not provide a ranging signal shortly and Galileo SOL has been designed for different purposes, so we will have to rely on user segment authentication services for a while.
- The GNSS authentication research community has dedicated the last 10 years to develop complex signal spoofing and signal authentication techniques, but it's time to get back to the problem: how do we authenticate PVT? The GNSS community wants a clear answer for every application.
- Whilst following the security life cycle, PVT threats and mitigations can now be categorized to begin a process of commercial receiver certification for PVT authentication.

Signal authentication options

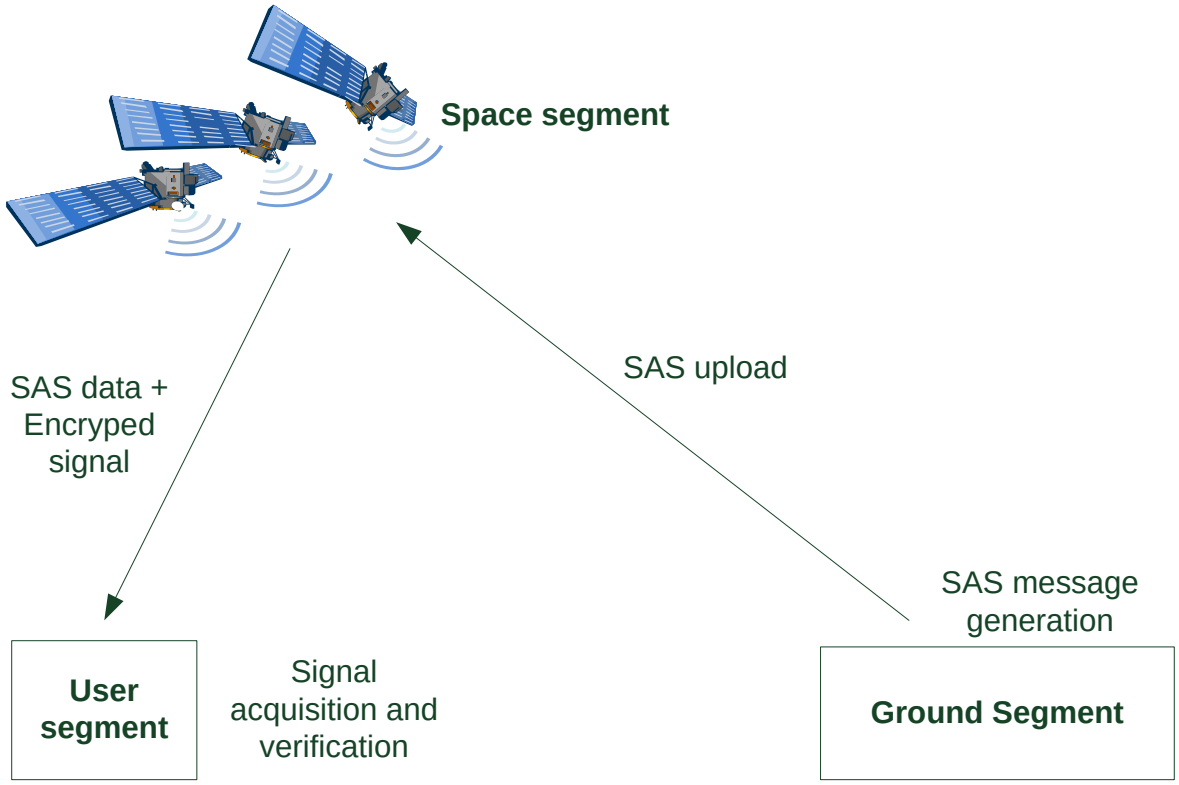
- **User Level**
  - Based only on receiver authentication techniques
  - Works on legacy systems that do not provide authentication
- **System level**
  - The system is designed for providing the service and the authentication service is embedded in the signal

User Level

- Autonomous
  - Monitoring of signal inconsistencies: pseudorange and time jumps, RAIM, antenna techniques
- Use of external sensors
  - IMU
  - Odometer, wheel speed for automotive (PUMA)
  - Signal of opportunity
- External aiding
  - Data verification via external provider (TIGER, STON)
  - Use of non deterministic signal (e.g. GPS P(Y) concept)

System Level

- Authentication at data layer
- Authentication at signal / spreading code layer

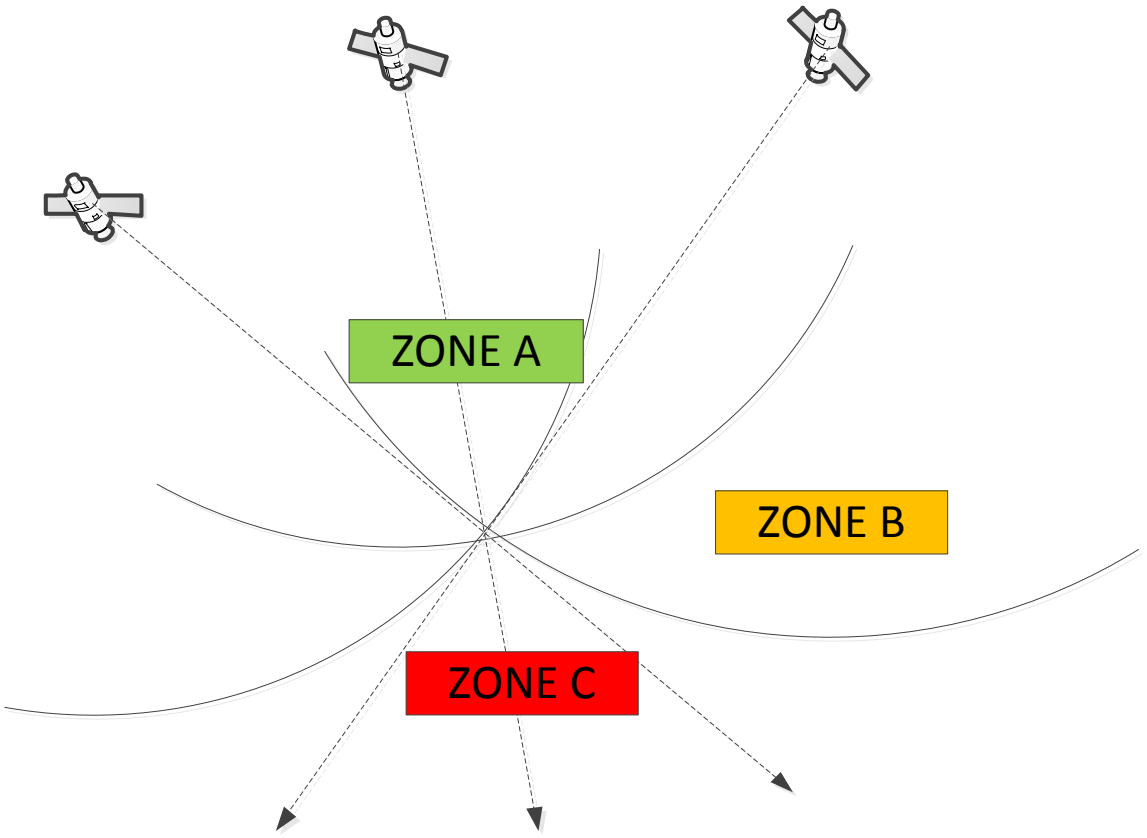


Data layer

- Navigation Message Authentication (NMA)
  - The difference from authentication in standard communication systems is that data in GNSS is used for ranging and timing
  - Requires trusted clock for full assurance
- Navigation Message Encryption (NME)

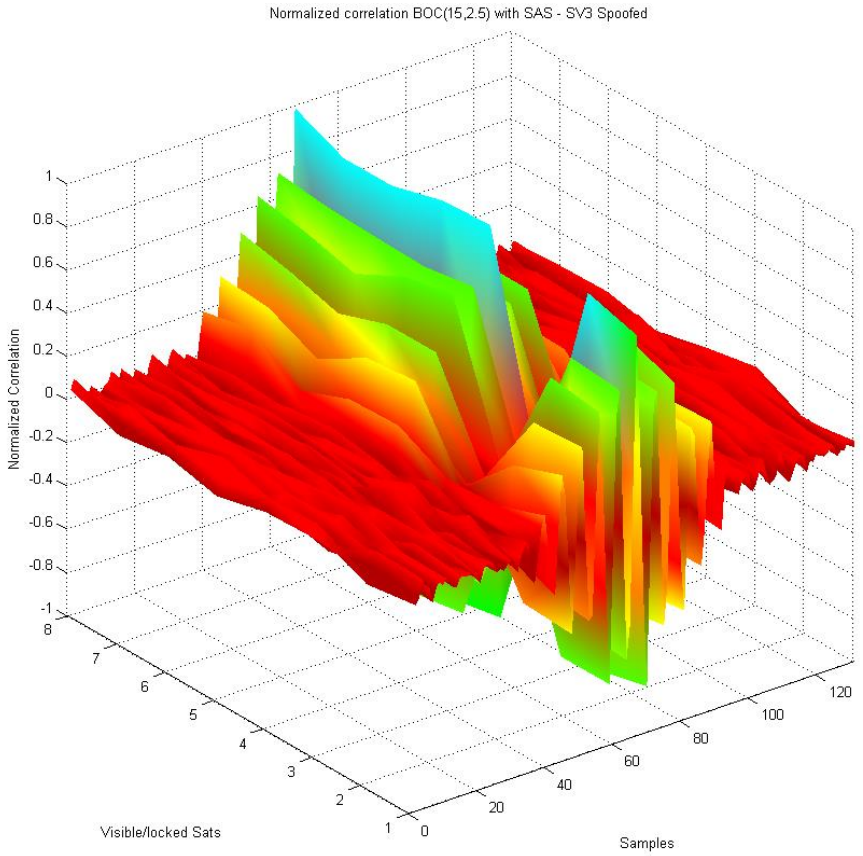
Issues with NMA

- Message overhead
- Key distribution
- Time to alert
- Data reuse



Signal and spreading code

- Spreading Code Encryption (SCE)
- Spread Spectrum Security Codes (SSSC)
- Signal Authentication Sequences (SAS)



Issues with signal level authentication

- SCE blocks signal access to users without keys
- SSSC could create issues with legacy signals
- SAS the best compromise but requires an open and encrypted signal

Conclusions

- While the research will continue towards new proposals for civilian signal authentication, the industry should have a plan B for the next 10 years, developing algorithms at receiver level.
- A task force should be created to give clear responses (security requirement standards) to the civilian GNSS community.

Example of security requirements for standardization of commercial receivers (E.g. FIPS 140-2 standard approach)

	Signal	Hardware	Software	PVT Data
Level 1	Anti Spoofing based on position solution algorithms	Integration of a trusted clock	firmware upgrade protection	Requires data authentication Data for authentication stored in flash memory
Level 2	Anti Spoofing based on position solution algorithms	Use of anti-tamper coating	firmware upgrade protection	Requires data authentication
	signal processing techniques (non predictable signals, SSSC, SAS)	Integration of a trusted clock		Data for authentication stored in flash memory
Level 3	Requires ranging from signal with Navigation Message Authentication (NMA)	secure memory	firmware upgrade protection	Requires data authentication
		Hardware acceleration	trusted boot ROM	Data for authentication stored in secure memory
		trusted clock		
Level 4	Requires ranging from signal with Spreading Code Encryption (SCE)	Tamper detection HW	firmware upgrade protection	Requires PVT data authentication and privacy
		data Zeroization		
		secure memory storage	trusted boot ROM	Data for authentication and privacy stored in secure memory
		Hardware accelerator		
		trusted clock		

Thank you

Oscar Pozzobon

Qascom S.r.l.

info@qascom.com

Qascom
Trust is Nice, Control is Better.