Malta Galileo Conference

# European GNSS Supervisory Authority (GSA)

# Security Department

## Governmental Applications of the Galileo System

## The Public Regulated Service

## Malta, 12 October 2010


***Olivier CROP***
***Head of Security***

+32(0)229 58426
Olivier.Crop@gsa.europa.eu

***Rodolfo Crescimbeni***
***PRS Officer***

+32(0)229 85170
Rodolfo.crescimbeni@gsa.europa.eu

# Topics

- Market Development of PRS & PRS Principles (OC)
  - 1 – Presentation of the GSA on Security and PRS
  - 2 – Introduction to the PRS
  - 3 – PRS Market
- Pilot Projects – FP7 and FP8 Opportunities (RC)
  - 4 - PRS Pilot Project
  - 5 – FP7 and FP8 Opportunities

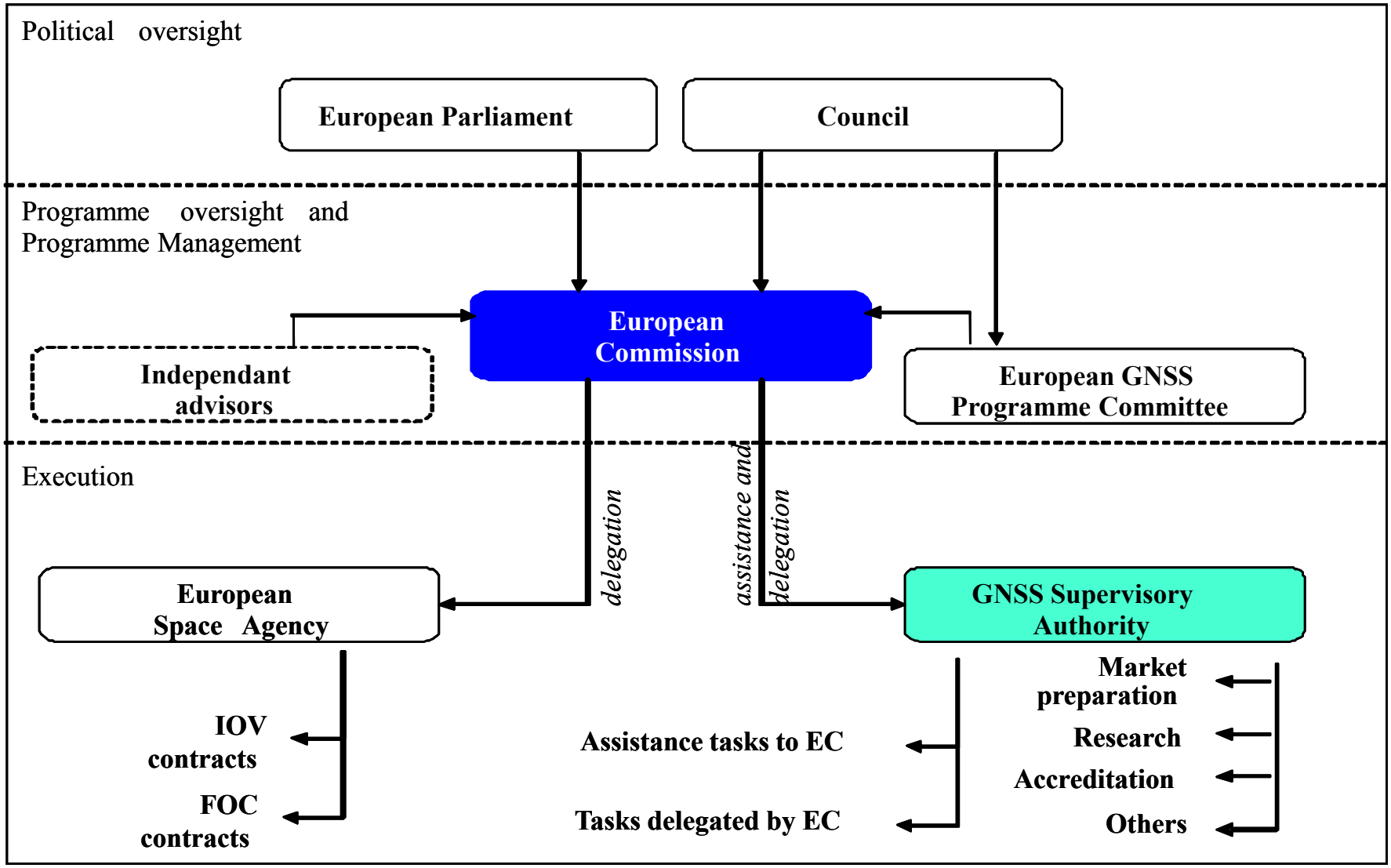
# Topics

- Market Development of PRS & PRS Principles (OC)
  - 1 – Presentation of the GSA on Security and PRS
  - 2 – Introduction to the PRS
  - 3 – PRS Market
- Pilot Projects – FP7 and FP8 Opportunities (RC)
  - 4 - PRS Pilot Project
  - 5 – FP7 and FP8 Opportunities

# What is the European GNSS Agency (GSA)?

- European GNSS Agency (GSA)
  - GSA is a community agency of the European Union with its own legal personality but governed by European public law
  - Created by the Council Regulation (EC) No 1321/2004 of 12 July 2004
  - Temporary seat in Brussels
- Role of the GSA under revision
  - Core responsibilities redirected in 2008 from Programme Management to Security
    - Security accreditation of the European GNSS Systems (Galileo/EGNOS)
    - Operation of the Galileo Security Monitoring Centre (GSMC)
  - Support to the Commission
  - Commercialisation of the systems
    - Promotion of applications and services
    - Ensure that the components of the systems are certified by the appropriate, duly authorised, certification bodies
  - New regulation should be enforced before EOY
    - Is currently known as "European GNSS Supervisory Authority"

# Galileo Programme Governance Structure



# GSA Towards The Operational PRS

- Confidence in System and Operational Security
  - Purpose of the Security Accreditation process
- Full Operational PRS Chain
  - Including not only the Galileo Sytem but all the specific facilities and operations to be set up
    - Galileo Security Center
    - National interfaces
- PRS Regulatory Framework
  - PRS Access Policy
  - PRS Common Minimum Standards
  - PRS Guidelines and Standards
- PRS Service Commissioning Phase (Pilot Project)
  - Through a dedicated pre-operational phase including notably
    - Exercise MS/GSMC interface
    - Initial experience with Galileo IOV
    - User Management Delegation
- PRS User Segment Development and PRS Market Boost
  - PRS Receivers
  - PRS Security Module
  - Application Demonstration

# Topics

- Market Development of PRS & PRS Principles (OC)
  - 1 – Presentation of the GSA on Security and PRS
  - 2 – Introduction to the PRS
  - 3 – PRS Market
- Pilot Projects – FP7 and FP8 Opportunities (RC)
  - 4 - PRS Pilot Project
  - 5 – FP7 and FP8 Opportunities

# Potential use in key areas makes the EU GNSS a Critical Infrastructure

- **Positioning**
  - Reporting the coordinates of hazardous goods, high value items, fleet management …
- **Navigation**
  - For critical transport, law enforcement, emergency services, defence …
- **Timing**
  - Systems and network synchronization for electricity, oil and gas distribution, telecom operators …

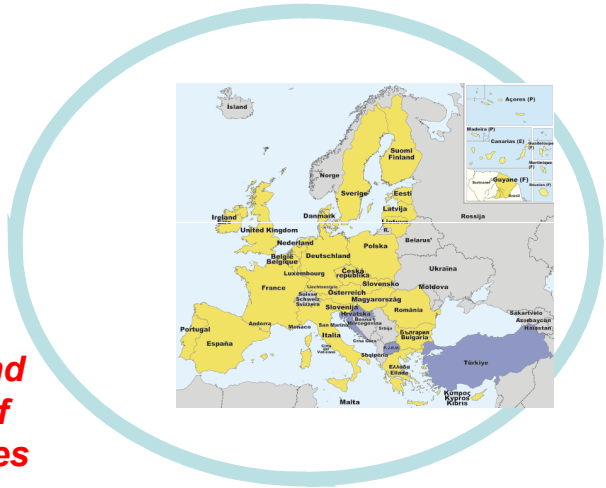
# Galileo Security Doctrine


PRS

*Accidental or deliberate attack on Galileo*

*③ Prevention of misuse of services*

- *Control of service denial*
- *Control of legitimate use*



*Illegitimate use*

*Subversive and hostile use of Galileo services*

*① Protection of Galileo infrastructure and*

*② Protection of all services*

- *Ensure availability*
- *Ensure integrity*
- *Ensure confidentiality*

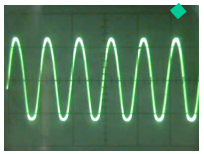
PRS

# GNSS signal weaknesses

Satellites

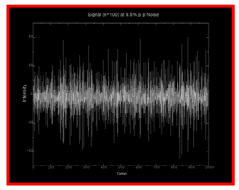
Navigation message

010110110011001

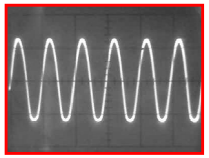


Carrier modulation

Jammer



010110110011001



Spoofer

## Receiver

**Synchronisation process on carrier modulation**

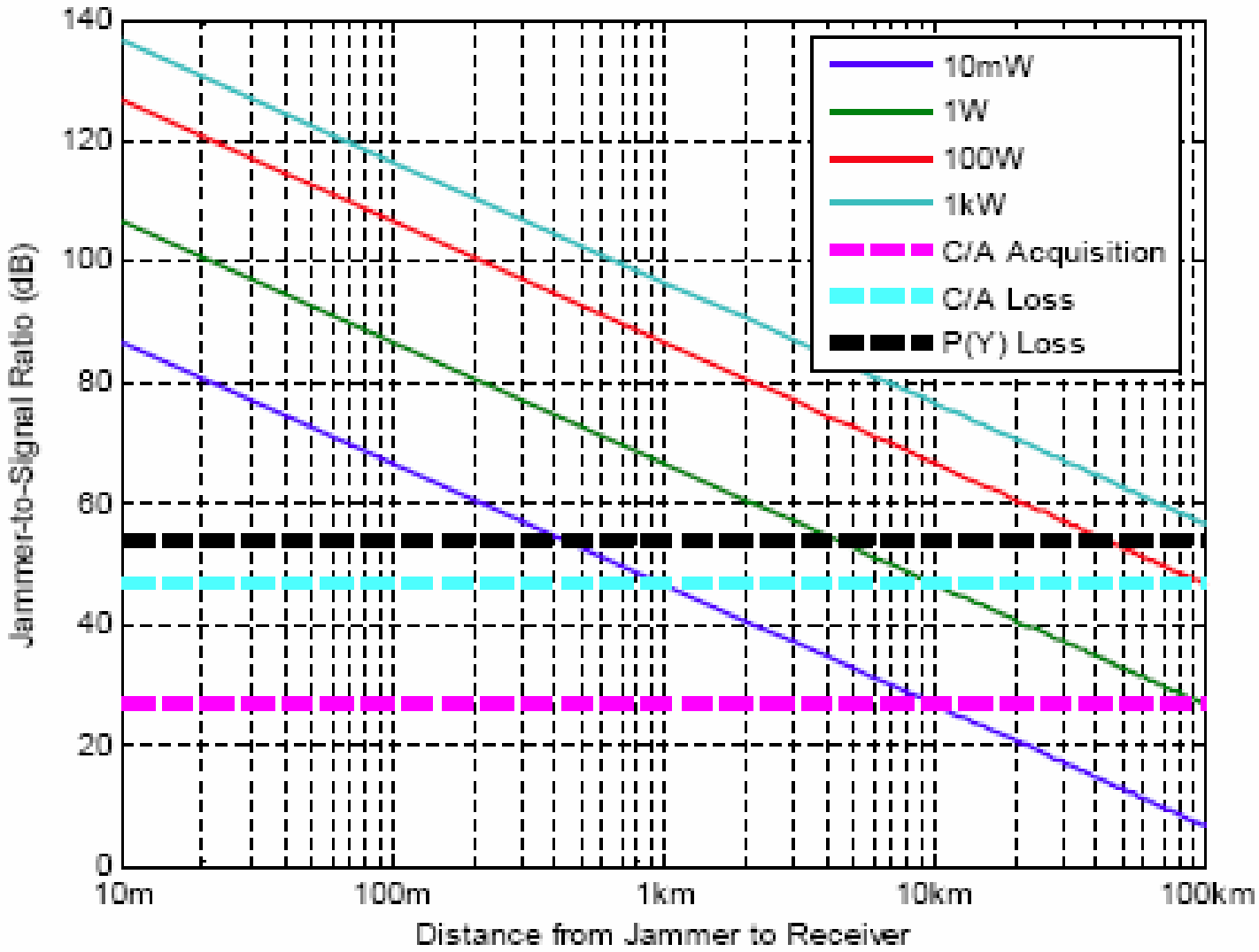
**Demodulation process of navigation data**

010110110011001

**Calculation of Position Speed Timing**

# Just a few available GNSS (GPS) Jammers …

# Susceptibility of GNSS to Interference/Jamming




Source: Roke Manor Research

# Why PRS?

- Several THREATS to GNSS services
  - Denial of service (DoS)
  - Spoofing
  - Misuse

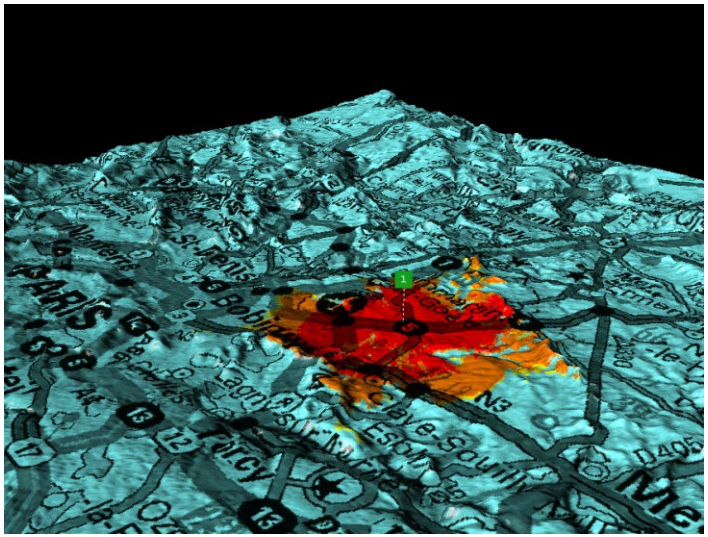
  → Against EU/MS interests
- Several security NEEDS for critical applications
  - Improved Continuity of Service
  - Authentication
  - Access Control

  → Provided by the PRS
- The need of continuity for PRS applications translates into two kind of measures
  - Measures on Galileo infrastructure assets, as a general rule

    ⇒Benefits to all Galileo services
  - Additional measures specifically designed to support PRS in case of direct attack

# Jamming threat and need for improved availability

- Signal power at reception side is very low
- Can be easily jammed by
  - Non-intentional RF interference
  - Intentional jamming
- Jamming is countered by
  - PRS signal
    - Wider band Signal
    - Band Diversity (L1 + E6)
  - Additional measures
    - Signal processing, hybridization techniques
    - Controlled Radiation Pattern Antenna (CRPA)
    - Spectrum monitoring, law and enforcement



# Spoofing threat and the need for Authentication

- GNSS signals can be generated and radiated so to make receivers calculate counterfeit and hazardous PVT
- GNSS spoofer is essentially a GNSS signal generator + transmitter element
- Spoofing is countered by crypto techniques
  - Crypto Key must be protected
  - PRS is encrypted and PRS keys are protected

# Misuse threat and the need for Access control

- Satellite navigation is a force multiplier
  - Providing more efficiency to command, control, communication, intelligence, accuracy of weapons
- When national security is threatened, it may be necessary to deny adversaries from any GNSS capability
- Access to GNSS shall be controlled by
  - Capability to deny by local jamming of all but controlled services
  - The access control to the PRS is performed via several means
    - Only users holding receivers with security module configured
    - Only PRS receivers holding operational keys
    - Denial orders can be sent to PRS receivers if and when compromised

# When and where is PRS needed ?

- If you can't accept , ANYWHERE and ANY TIME, the impact on CRITICAL applications of an UNFORESEEN attack on Galileo signals, especially using
  - Hostile jamming
  - Hostile spoofing

- If you need to LOCALLY and TEMPORARY, PREVENT the possible hostile use of Galileo services, with
  - Volontary area denial (by jamming) of Galileo services without governmental control of legitimate use

- PRS is the only way to ensure service continuity
  - Navigation
  - Localisation
  - Timing
  - Synchronisation

# Day to day possible PRS use (1st case)

*Questionnaire to the EU Member States on the use of PRS, Issue 1 – 3 May 2006*

| | |
|---|---|
| A | Internal security |
| B | Law enforcement |
| C | Custom |
| D | Critical transport |
| E | Critical energy |
| F | Critical telecom |
| G | Strategic econcomic and commercial activities |
| H | Emergency services |
| I | Defense |
| J | Miscellaneous - others |

- If you can't accept , ANYWHERE and ANY TIME, the impact on CRITICAL applications of an UNFORESEEN attack on Galileo signals, especially using
  - Hostile jamming
  - Hostile spoofing

- PRS is the only way to ensure service continuity
  - Navigation
  - Localisation
  - Timing
  - Synchronisation

*Reference :*
*« PRS concept of operation », Issue 1.0 – 05/04/2005*

# Possible PRS use in specific situations (2nd case)

*Intelligence on Potential threat*

*Area denial by jamming*

*End of jamming*

***You want to prevent a possible hostile use of Galileo services in a specific area, for national security reasons***

- **If you need to LOCALLY and TEMPORARY, PREVENT the possible hostile use of Galileo services, with**
  - **Volontary area denial (by jamming) of Galileo services without governmental control of legitimate use**

*Threat*

*Area protected by « official » jamming. PRS is then the only available service (and also protected against hostile jamming or spoofing)*

*Outside of the area, all the services are maintained*

# Galileo PRS and its Benefits (1)

- PRS - An encrypted, access controlled GNSS service transmitted from all Galileo satellites
  - Strong access control to (through PRS key management)
  - Strong security control of the PRS management chain
  - Security services provided over-the-air & via MS PRS infrastructure
  - User management through PRS orders transmitted via the PRS SIS
  - In accordance with the PRS Access Policy being developed by EC Member States

- PRS - A service with an increased probability of continuous availability
  - A sovereign EU GNSS service under the direct control of EU Member States complementing other GNSS systems
  - Independence from other GNSS
  - Spectral separation from other Galileo signals
  - Multi-frequency
  - Improved availability when used in coordination with other GNSS (e.g. PRS/GPS)

# Galileo PRS and its Benefits (2)

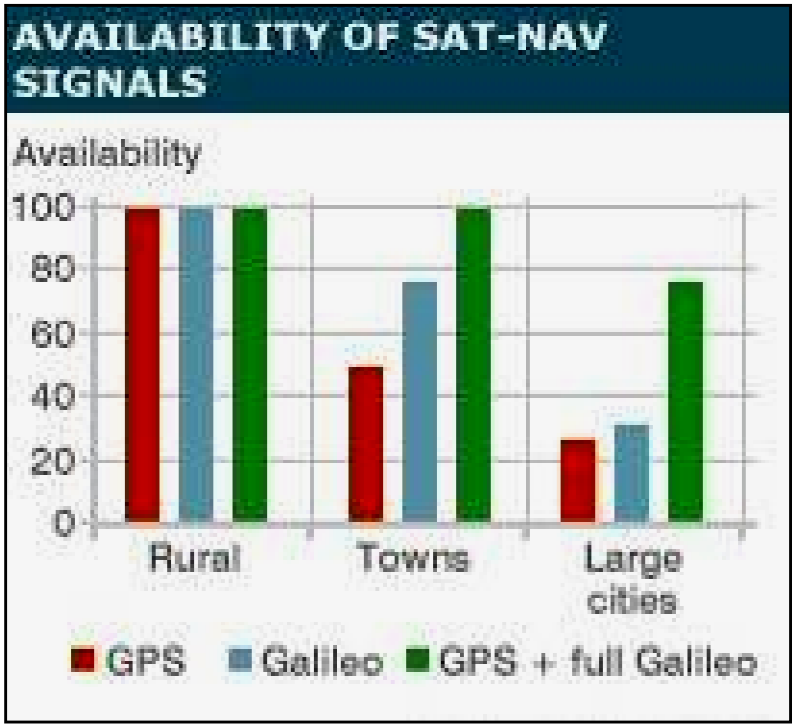
- PRS - providing higher levels of protection against threats to the SIS than can be provided for open services
  - Through PRS signal design (anti-spoofing, signal authentication)
  - Through the use of enhanced receiver anti-interference capabilities
  - Potentially through future additional measures to coordinate detection, identification and removal of interferers (cf PROTECTOR)

- PRS - Good navigation/timing performance
  - Higher expected accuracy, due to the signal modulations adopted
  - Good stand-alone performance which can be improved when used in coordination with other GNSS signals (e.g. GPS/PRS)

- PRS - Availability of PRS User Equipment
  - Indigenous European production of security certified PRS receivers avoiding complex international export agreements.

# Benefits of Multi-GNSS Operations

- Multi-GNSS Benefits
  - Improvements in Availability
    - especially in difficult reception environments
  - Improvements in Accuracy



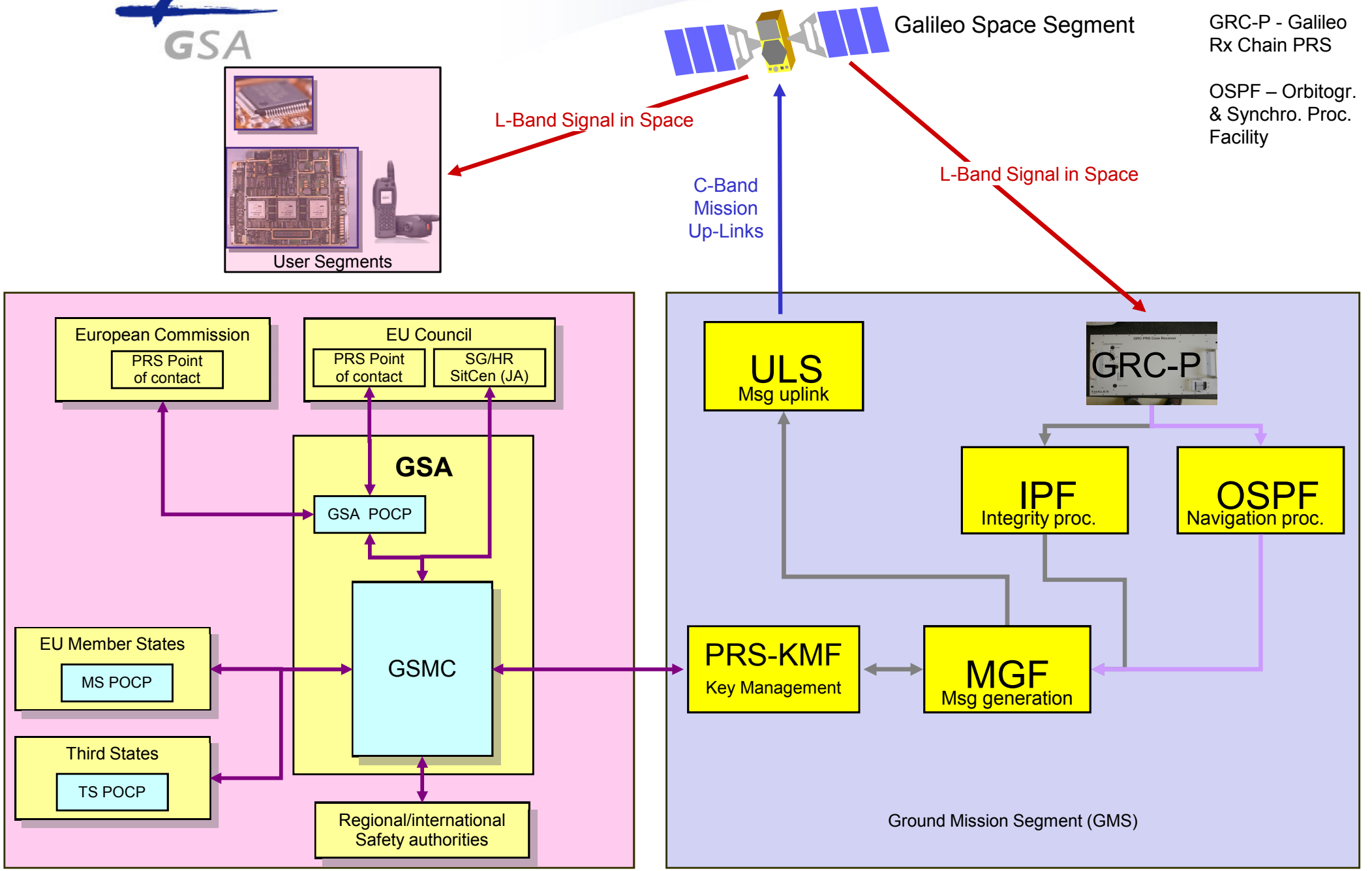

*Dual Constellation Improvements in Availability*

| | L1A GALILEO PRS | L1 GPS M-CODE | COMBINEDGALILEO/ GPS L1 RECEIVER | COMBINEDGALILEO/ GPS RECEIVER |
|---|---|---|---|---|
| Horizontal | 3.97 m | 3.97 m | 1.65 m | 0.34 m |
| Vertical | 7.94 m | 7.94 m | 3.31 m | 0.69 m |
| 3D-P | 8.94 m | 8.94 m | 3.71 m | 0.77 m |

[redacted]. Typical Accuracies for the Galileo PRS, GPS M Code and Combined Positioning

*Dual Constellation PRS + GPS M-Code Improvements in Accuracy*

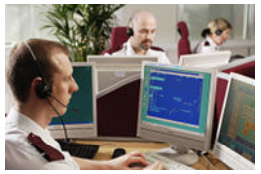
# PRS Chain Architecture



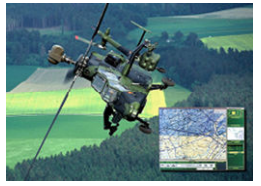
- Market Development of PRS & PRS Principles (OC)
  - 1 – Presentation of the GSA on Security and PRS
  - 2 – Introduction to the PRS
  - 3 – PRS Market
- Pilot Projects – FP7 and FP8 Opportunities (RC)
  - 4 - PRS Pilot Project
  - 5 – FP7 and FP8 Opportunities

# Who will the PRS users be? PACIFIC Results (1)

| Application Domains | Main operational scenarios and applications |
|---|---|
| • **Law Enforcement**<br>– **Police**<br>– **Special Ops**<br>– **Customs** | • Day to day patrolling coordinated by a control centre<br>– Navigation/Positioning for Land vehicles & Handsets<br>• Particular security measures enforcement<br>– During particular events (Olympics, G8 Summit…)<br>– Involving various kind of platforms<br>– Tracking of suspects' profiles, dangerous goods |
| • **Emergency Services**<br>– **Fire Brigades**<br>– **Ambulances**<br>– **Civil Protection** | • Coordination of land vehicles<br>– Automatic Vehicle Location (AVL)<br>– poss. Navigation<br>• Location of emergency personnel<br>– Navigation information for the unit<br>– Reporting of position & status for the control centre |
| • **Defence**<br>– **Army**<br>– **Marine**<br>– **Air Force** | • Various types of applications & platforms<br>– As a backup: Navy vessels, some aircraft…<br>– As a Sole Mean: Infantryman equipment, some synchronisation applications…<br>– As a setting mean for other PNT systems: Helicopters… |

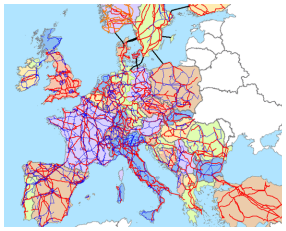






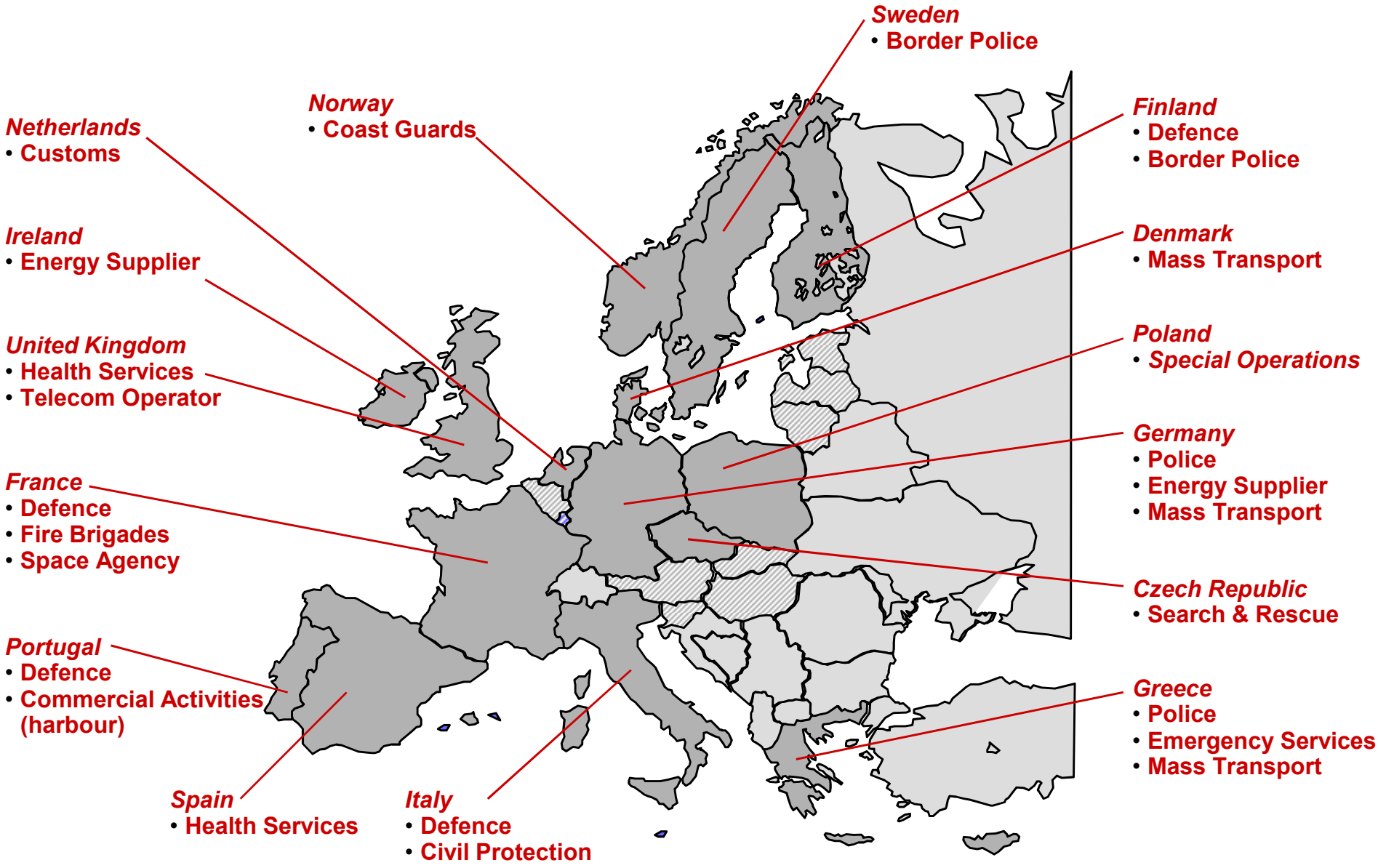

Note: This list of potential applications is based on inputs from users.
Each Member State will be responsible for authorising its users and applications for PRS.

# Who will the PRS users be? PACIFIC Results (2)

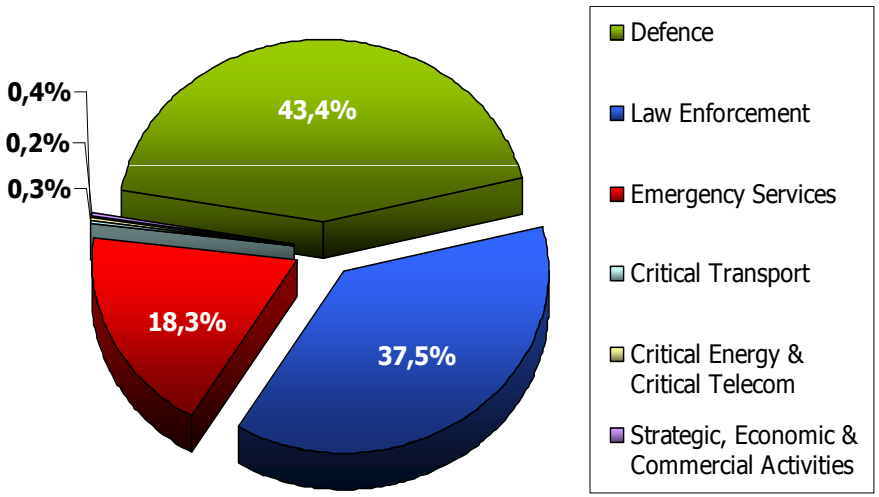
| Application Domains | Main operational scenarios and applications | |
|---|---|---|
| • **Critical Telecom**<br>– **Network Operators** | • Network synchronisation and timing<br>– GNSS as primary reference clocks (backed with atomic clocks)<br>– Frequency calibration of radio signals (GSM base stations) |  |
| • **Critical Energy**<br>– **Energy Suppliers** | • Network monitoring and control through PMUs<br>– Internal oscillator management<br>– Time stamping of incident<br>– Synchronised measurements |  |
| • **Critical Transport**<br>– **Civil Aviation** | • None applications identified for PRS due to certification & security constraints |  |
| • **Strategic Activities**<br>– **Commercial Ports**<br>– **Space Agencies** | • Commercial ports<br>– Vessel traffic management<br>– Container tracking & tracing<br>• Space agencies<br>– Positioning of spacecraft (orbit control & restitution)<br>– Synch. of on board clocks & comm. links |  <br>  |

Note: This list of potential applications is based on inputs from users.
Each Member State will be responsible for authorising its users and applications for PRS.

# PACIFIC Study: Selected 15-25 UCs subset



# PRS Market – Addressable Market

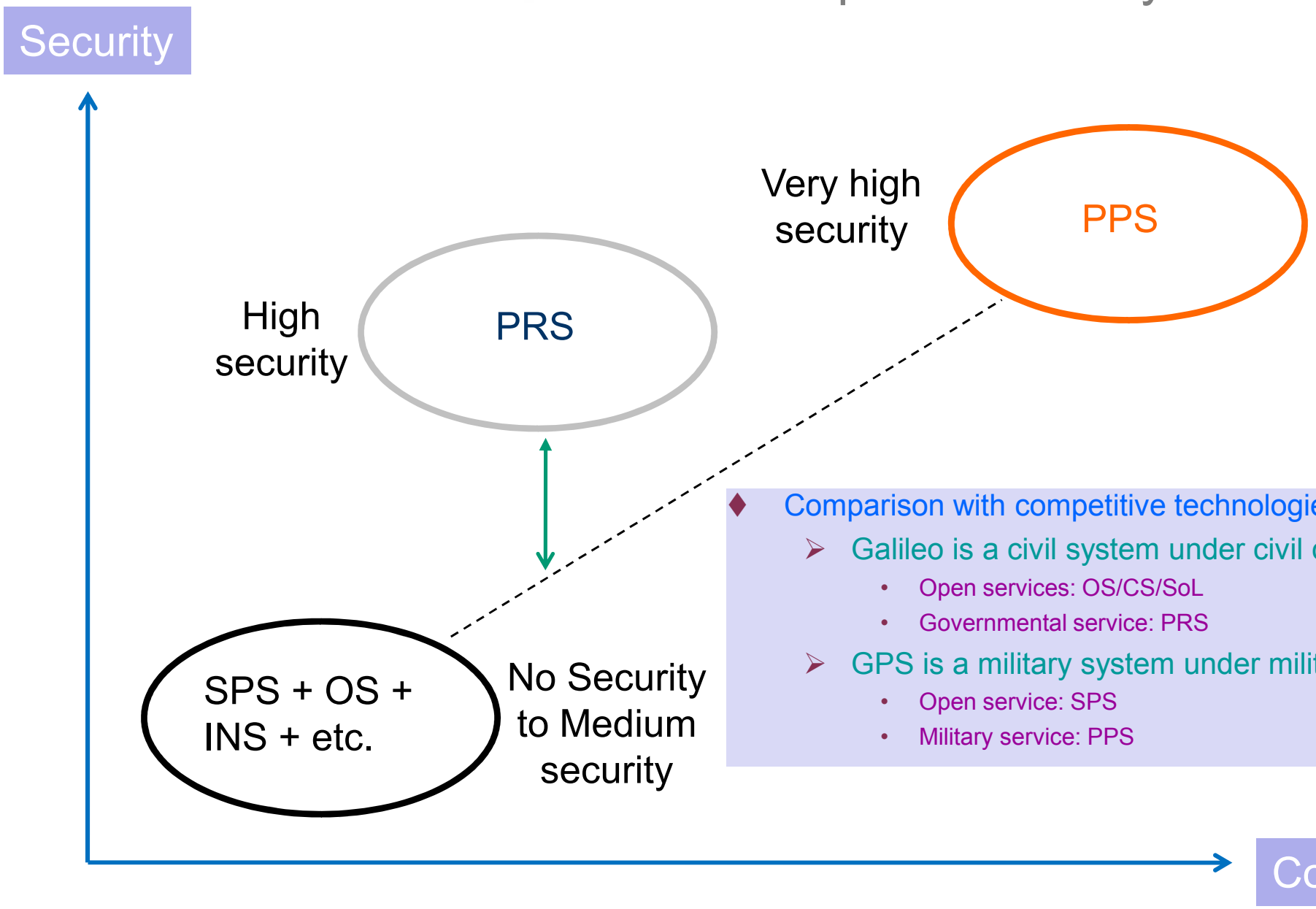



| | |
|---|---|
| **Defence** | **1 791 944** |
| **Law Enforcement** | **1 548 459** |
| **Emergency Services** | **754 971** |
| Critical Transport | 16 750 |
| Critical Energy & Telecom | 13 600 |
| Strategic, Economic & Commercial Activities | 7 265 |
| **Total** | **4 132 989** |

- PRS may bring benefits for numerous Users in various Applications Domains
- Market Boosters are
  - Defence
  - Law Enforcement & Emergency Services (especially PMR users)
- 80% Low End Core receiver
- 20% High/Medium End Core Receiver

- Best case if
  - Dual-mode receivers (Galileo + GPS)
  - Additional cost per unit is < 100€
  - PRS is compliant with PMR management

# PRS To Improve Security/Cost Ratio




- Comparison with competitive technologies
  - Galileo is a civil system under civil control
    - Open services: OS/CS/SoL
    - Governmental service: PRS
  - GPS is a military system under military control
    - Open service: SPS
    - Military service: PPS

# Thank you for your attention