

# Job Title: Galileo G2 Key Management and Crypto Engineer

Job Requisition ID 10901 - Posted 10/11/2020



## EUROPEAN SPACE AGENCY

Vacancy in the Directorate of Navigation.

ESA is an equal opportunity employer, committed to achieving diversity within the workforce and creating an inclusive working environment. Applications from women are encouraged.

### Post

#### Galileo G2 Key Management and Crypto Engineer

This post is classified A2-A4 on the Coordinated Organisations' salary scale.

### Location

ESTEC, Noordwijk, The Netherlands

### Description

Galileo G2 Key Management and Crypto Engineer in the Galileo Second Generation System Security Service Unit, Galileo 2nd Generation Project Office, Galileo Programme Department, Directorate of Navigation.

### Duties

You will be responsible for overall activities related to Key Management and Crypto Engineering for Galileo Second Generation, including the definition and consolidation of requirements, as well as their verification, validation, qualification and certification. You will establish and coordinate activities under the Programme and with industrial consortia, and liaise with internal Agency entities and external ones in carrying out your duties.

Your responsibilities, within project boundaries and constraints, and under the supervision of the Head of the Galileo Second Generation System Security Services, will include:

- Leading the definition, analysis and consolidation of Key Management and crypto requirements for the whole Galileo 2nd Generation Project, including system, space and ground segment. This covers both classified and unclassified aspects, for which close coordination with the G2G System Engineering Services will be required;
- Supporting the implementation of overall security engineering, including security requirements flow-down, implementation follow-up, security operations engineering and maintenance of the Galileo Evolutions Mission Security Baseline, with the main focus on the Key Management and crypto requirements of the Galileo Evolutions System Security Requirements (eSSRS);
- Supporting the definition and maintenance of the technical security requirements (functional, performance and operational) applicable to procurement of the overall G2G system infrastructure;
- Leading the definition of the Key Management and crypto verification, validation, qualification and certification activities, in support of the overall qualification of the security requirements at System and Segment level (space and ground);

### Duties continued

- Contributing to, and leading when required, the definition and implementation of tools and testbeds to demonstrate, prototype, and validate the G2G Key Management and Crypto design and requirements;
- Contributing to the G2G system architecture and operations concept in the areas of Key Management and crypto;
- Coordinating with the Space Segment team, and the Ground Segment team in the areas of Key Management and crypto, supporting procurement of the security equipment on-board satellites and within the ground segments;
- Supporting the correct implementation and technical end-to-end consistency of the Key Management and crypto requirements for the G2G Project;
- Supporting preparation of the G2G core infrastructure;
- Supporting preparation of documentation required by the SAB for the accreditation process;
- Supporting the Agency's interactions with the National Expert Team Working Group, TEC WG, the SPECIAL PRS WG, the Security Accreditation Panel (GSAP) and the Crypto Distribution Authority task force (CDA TF) in the area of Key Management and Crypto;
- Supporting G2 Public Regulated Service (PRS) engineering with regard to key management, access control and crypto aspects;
- Supporting implementation of the G2G Advanced PRS IOC and FOC Services, including completion of the associated system infrastructure and service milestones, as well as the corresponding service validation activities;
- Generating lessons learned and contributing to Knowledge Management initiatives in the Directorate of Navigation;

- Supporting R&D activities in Key Management and crypto under the Galileo 2nd Generation Project, EGEP, H2020 & Horizon Europe Programmes.

In the execution of your tasks, you will, at technical level, coordinate the industrial support team in charge of G2G Key Management and Crypto Engineering and cooperate closely with the other team members working on System Security design and verification. You will also cooperate with Space Segment, Ground Segment, Operation support and other teams in the Directorate of Navigation, the Technical Directorate and ESA.

## Technical competencies

Knowledge and Experience in Key Management and crypto engineering  
Knowledge and Experience in System & Security Engineering  
Knowledge and Experience in Satellite navigation system and related security architectures  
Knowledge and Experience in managing industrial contracts

## Behavioural competencies

Integrity  
Problem Solving  
Teamwork  
Results Orientation  
Planning & Organisation  
Customer Focus

## Education

A Master's degree in telecommunications engineering or similar is required.

## Additional requirements

In-depth knowledge of Security and GNSS system is required.  
You should be able to coordinate, monitor and lead the engineering support provided to the Project in the relevant areas of expertise. You should be able to demonstrate that you can work in a fast-paced environment and handle pressure as may typically occur in a project team. You should be able to set priorities and to present practical solutions both verbally and in writing.  
You should have interpersonal and communication skills. You should have the ability to work autonomously, effectively and cooperatively in a diverse, international team environment, defining and implementing solutions in line with team and individual objectives and project deadlines. You should also have good technical, analytical, organisational and reporting skills, a proactive attitude to solving problems and an interest in innovative technologies.  
You should be ready to obtain security clearance from the national relevant authority. Already having security clearance is an asset.

## Other information

For behavioural competencies expected from ESA staff in general, please refer to the ESA Competency Framework.

The working languages of the Agency are English and French. A good knowledge of one of these is required. Knowledge of another Member State language would be an asset.  
The Agency may require applicants to undergo selection tests.

## The closing date for applications is 09 December 2020.

If you require support with your application due to a disability, please email [contact.human.resources@esa.int](mailto:contact.human.resources@esa.int).

-----  
Please note that applications are only considered from nationals of one of the following States: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the United Kingdom and Canada, Latvia and Slovenia and in addition of Member States of the European Union not members of ESA: Bulgaria, Croatia, Cyprus, Lithuania, Malta and Slovakia.

According to the ESA Convention the recruitment of staff must take into account an adequate distribution of posts among nationals of the ESA Member States. When short-listing for an interview, priority will first be given to internal candidates and secondly to external candidates from under-represented Member States. (<http://esamultimedia.esa.int/docs/careers/NationalityTargets.pdf>)

In accordance with the European Space Agency's security procedures and as part of the selection process, successful candidates will be required to undergo basic screening before appointment.

Recruitment will normally be at the first grade in the band (A2); however, if the candidate selected has little or no experience, the position may be filled at A1 level.