EDF-2021-SPACE-D: Resilient space-based PNT and SATCOM

- **EDF-2021-SPACE-D-EPW:** European protected waveform and accompanying technologies for resilient satellite communications against jamming.

This call aims at improving space-based PNT resilience in contested environments through the mapping and analysis of threats. It will complement the on-going EDIDP project on Galileo PRS receivers and contribute to reinforce Galileo as a credible European solution for defence applications.

This call aims also at accompanying the development of European technologies and products for interoperable and resilient military satellite communications.

Proposals are invited against any of the following topics

- **EDF-2021-SPACE-D-EPW:** European protected waveform and accompanying technologies for resilient satellite communications against jamming.

Budget

The Union is considering a contribution of up to EUR 50 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and main functional requirements.

Several actions, addressing different topics, may be funded under this call.

The Commission will pay particular attention to existing and on-going developments within the Union to avoid unnecessary duplication.

Space is one of the global commons and an emerging operational domain at the same time. It provides unique options to deploy capabilities, which deliver services increasingly indispensable for military purposes and operations. This situation is going to produce specific new threats and challenges. The access to space has to be duly monitored and eventually protected as well as the capabilities already deployed and operating in orbit.

In today's military applications supported by satellite communications, security, resilience, information assurance and link efficiency technologies are inextricably linked. Military operations are becoming more complex as conflict areas grow more dispersed on a global scale, with a growing need to support a diversity of on-the-move, on-the-pause and fixed platforms. At the same time, security threats are becoming more apparent, raising concerns that nations, terrorist groups, criminals and individual hackers can jam, interrupt and endanger military operations. The challenge is to meet, in a secure and guaranteed way, the increased demand for raw capacity generated by continuous growth in space data rate requirements for military purposes. This covers the trend of higher mobility as well as the filling of current coverage gaps (*e.g.* over the Polar Regions).

Specific challenge

The complexity of diverse and dispersed military operations translates into requirements to have access to complex global satellite communication networks with a mix of different

satellite constellations, networks and services to support a wide variety of military applications. Security and resilience, as key features in today's military use of space, have to be paired with efficient technologies in order to cope with the increased data demand through high-bandwidth consuming services that need to be supported by satellite communication, such as ISR and situational awareness, the growing use of drone applications, and the need for seamless and real-time end-user connectivity during operations. However, these wide-ranging and complex requirements face an increased risk of ill-intentioned acts including cyber- attacks against military satellite communication networks such as jamming, signal detection and spoofing and interception attempts.

The key element to tackle these security challenges is the implementation of an integrated multi-layered security and resiliency approach for next-generation defence satellite networks with a fully European protected waveform and accompanying technologies for satellite communications resilient against ill-intentioned acts. This European Protected Waveform (EPW) must respond to the operational requirements and the identified security challenges, and considerably enhance interoperability during joint operations with allies whilst assuring seamless operations and protection of the satellite link.

The great majority of Member States do not have autonomous access to secure satellite communication waveforms, although they also engage in military operations in a national or multinational context (EU, NATO, UN peacekeeping, *etc.*). The investment for developing a protected waveform cannot be carried out by a single nation alone and requires a multinational development approach in a European context with the aim to establish an interoperable European Protected Waveform.

The European Protected Waveform is fully in line with and would contribute to the EU ambition to set up resilient satellite communication services for governmental and institutional security users and to achieve increased EU autonomy in space, as outlined in various documents from the Space Strategy for Europe, to the EU Global Strategy and the current EU Space Programme for 2021 to 2027. In the EU Capability Development Plan (CDP) of 2018 space has been identified as one of eleven EU capability development priorities. Following the CDP, in the Strategic Context Case for Space Based Information and Communication Services, established with and approved by the EDA participating Member States, a European Protected Waveform has been identified as a gap and the development of an EPW has been agreed as a short-time activity to fill this gap. More recently, in the Commission Action Plan on synergies between civil, defence and space industries satellite based secure communications and connectivity was again identified as a key activity and future flagship action with focus on standardisation and innovation, aiming at providing a 'resilient connectivity system allowing Europe to remain connected whatever happens, including large-scale cyber-attacks'.

Scope

The proposals should address the development of an EPW for satellite communications as well as the complementary ancillary technologies addressing security and resilience that can be used by different EU Member States individually or together in a joint operational context (EU, NATO, multi-nation missions).

The EPW must be able to operate in the complex military operational environment described in the specific challenge and bring a solution to the corresponding challenges. The proposals must not be limited to the work towards the development of a waveform but must also include

complementary ancillary technologies to provide an integrated multi-layered security and resilient approach to military satellite communications.

The proposals must keep the following five (5) key considerations in mind:

1/ Innovation

The EPW development must not just be a copy and paste of existing waveform solutions, licenses and technologies. The proposed EPW must be ambitious and innovative, combining the individual strengths of different Member States or associated countries and of different members of the European satellite communication industry. The EPW program must be open to support future requirements and capability needs.

2/ European autonomy and cooperation between Member States

The EPW must be capable of increasing the autonomy of the Union and of reducing the dependence on non-European satellite communication technology for military operations with mission critical and sensitive information. At the same time, it must allow for interoperability between Member States in a joint operational context in order to exchange mission critical information and improve the efficiency of the operations.

3/ Affordable and efficient satellite services

The EPW must be affordable and include the most efficient satellite communication waveform, networking and equipment technologies to reduce OPEX (*e.g.* bandwidth, planning resources) and CAPEX (equipment cost) compared to current existing expensive (proprietary) military satellite solutions. The EPW must include already available innovative Commercial Off-The-Shelf (COTS) satellite communication technologies (*e.g.* DVB-S2X waveform standard) in combination with the latest security and resilience technologies. There must no longer be a trade-off between the efficiency of the waveform and security. As such, high throughput demands must be achieved even with small satellite terminals using a limited amount of satellite bandwidth (in contested and/or congested environments).

4/ Flexibility and scalability

The EPW must be portable on different software defined modems with different form factors (board, modem, terminal), different platforms (fixed, on-the-move, on-the-pause) and be used across multiple types of satellite communication networks, different types of multi-orbit satellite constellations (LEO, MEO ,GEO, HEO, high- and very-high throughput satellites, spot beams, regional and global beams) and different network architectures (VSAT, point-to- point, mesh) also considering possible extension to future EPW processed satellite transponder employment. At the same time, the EPW must be operational in different satellite frequency bands (at least C-band, X-band, Ku-band and (mil- and civ-) Ka-band) with extension to Q-/V-band to support future military constellations of communication satellites and exchange, broadcast, multicast, unicast or relay a large range of satellite services and applications from low to very high data rates. Interrelations with the ESSOR (European Secure Software defined Radio) project must be investigated in order to avoid unnecessary duplications and maximise synergies between these projects.

5/ Multi-layered security and resilience

The EPW must be embedded in an integrated multi-layered secure and resilient approach to increase the protection of mission critical military satellite networks. Based on different threat analysis and Concept of Operations (CONOPS) scenarios, the EPW development must focus on building satellite networks that are resistant to the increasing security threats in terms of jamming, interference, interception and cyber. In addition, satellite link outages caused by rain fade, atmospheric conditions or on-the-move communication challenges must be reduced to a minimum. The EPW activity must investigate how different security levels can be offered towards different military end users depending on their security requirements and their daily operations (as well as the budgets available).

The scope must be extended to anti-jam, multi-band/multi-frequency terminals, network diversity and network security technologies to ensure end-to-end secure and resilient military satellite networks, fostering the possibility to exploit dedicated EPW processed transponders (e.g. on board frequency de-hopping, re-hopping capability) in order to even protect user access to satellite resources.

Targeted activities

The proposals must cover the following activities as referred in article 10.3 of the EDF Regulation, not excluding possible downstream activities eligible for development actions if deemed useful to reach the objectives:

- Studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- The design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment.

In particular, the proposals must cover the following tasks:

• **Study** Phase:

- Feasibility study, use cases, and CONOPS definition.
- Threat and vulnerabilities assessment, risk analysis, and identification of counter measures and security requirements (*e.g.* anti-jamming, network diversity, multi-band/multi-frequency terminal and network security solutions).
- System specification, Detailed Requirements Review (DRR) and architecture definition; benchmarking of existing solutions in the market.

• **Design** Phase:

- Detailed design of the system, including the Preliminary Design Review (PDR) and finishing with the Critical Design Review (CDR).
- Development of an EPW simulator to de-risk the development of subsequent technological demonstrators.
- The development of small-scale technological demonstrators to support decision making during the design phase. The demonstrators must:

- Demonstrate the functionality of the waveform used in different operational use cases alongside the adjacent security and resiliency technologies (multi-frequency terminals etc.) allowing testing against multiple instances of interference, jamming and interception etc. but also in context of different satellite types, different architectures, and platforms (on-the-move, on-the-pause and fixed). The use of drone technology to test the terminal and waveform technology is encouraged.
- Reproduce the operational environments in terms of usage and threats;
- Be set-up initially a lab environment, but should then be followed by a real satellite test with outdoor satellite terminals simulating operational use cases. Military end-users should be invited to witness the demonstrations and to provide feedback;

The end state must be an EPW standard for satellite communication, a so-called Blue Book, comparable to other communication waveform standards that can be implemented by industry on their baseband solutions (terminals, modems) and integrated in the Member States military networks. It must take into account the accompanying anti-jamming, network diversity, multi-band/multi-frequency terminal and network security solutions, based on traditional and new generation satellite systems that could implement the EPW communication standard in SW defined radio solution on board.

Functional requirements

In accordance with this integrated multi-layered security and resiliency approach for military satellite networks the EPW development should fulfil requirements at the level of the waveform, the satellite baseband equipment (terminals, modems, hubs, networks) and end-to-end satellite network level including multi-band/multi-frequency terminals, anti-jamming technologies, interference mitigation, network diversity, network security and cyber technologies. The demarcation point is the edge router of the satellite network which connects the hubs, gateways and modems with outside networks or the internet. With this approach it will be feasible to implement the EPW also on existing and operational telecommunication satellites.

• ***Protected waveform requirements:***

The EPW should:

- Be defined as a standard to enable interoperability in joint operations. Multiple terminal vendors should be able to support the EPW and be compatible;
- Be affordable, based on the best practices of COTS and government or military-grade waveforms;
- Implement the most efficient SATCOM technologies to obtain the best performance out of a satellite link;
- Support a range of different multi-orbit satellite constellations ((V)HTS, wideband, military, commercial, government, GEO, MEO, LEO), satellite architectures (pure transponder, partially or fully processed) and frequency bands (C-band, X-band, Ku-band, (mil- and civ-) Ka-band) with extension to Q-/V-band to support future milsatcom constellations) and have the capability to roam across the different satellite networks in a seamless manner;
- Be easy to port on other Software defined modems or hubs;

- Flexible to support multiple governmental and defence applications that require different levels of security;
- Consider a growing amount of on-the-move and on-the-pause platforms connected over the satellite with a need for mobility features (Doppler compensations, spreading modulation, small and flat antenna support, beam switching, beam hopping, etc.);
- Operate in GNSS-denied environments;
- Provide adequate protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping (Low Probability of Detection - LPD/ Low Probability of Interception LPI);
- Masking and obscuring traffic anti-jamming patterns across the satellite link that could give away activity related information on ongoing operations and assets.
- Consider a wide range of throughput requirements and satellite bandwidth sizes (symbol rates);
- Offer seamless and resilient satellite links against fading effects, interference (intentional and unintentional), shadowing effects and jamming (fixed and sweeping);
- Be capable of supporting different service models such as pooling and sharing.

• ***Multi-layered security & resilience requirements (extended capabilities):***

- The EPW is embedded in an integrated multi-layered security and resilience approach which increases the protection of mission critical military satellite networks. As such an overall approach needs to be envisaged to align the EPW development with the complementary security and resiliency technologies for ground and space segments.
- Anti-jamming technologies that allow to detect, mitigate, prevent and predict jamming efforts by 3rd party adversaries. This can be tackled through spectrum monitoring, geolocation and network management technologies working together with nulling or interference excision technologies as well as Anti-Jam waveform capabilities as Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum and beam forming technologies.
- Network diversity, redundancy and geo-redundancy technologies to increase the resilience of the military satellite network as well as multi-access capabilities (hybrid LTE/5G/etc.) with intelligent routing.
- Multi-frequency terminals and antenna systems that can dynamically steer its radiation pattern accordingly to connect to another satellite in a different frequency and satellite orbit to increase network resiliency. Both fixed, on-the-move and on-the-pause terminals, manpack and antenna systems need to be considered as well as different types of antenna technologies (e.g. parabolic, electronically steered, phased array, flat antennas, etc.). The secure connection and interface between antenna system and baseband needs to be taken into account as well.
- Network and ground segment technologies that improve the cyber hardening of all satellite platform elements including protection against possible hacking, network intrusion, etc.
- Protection technologies against hostile action (e.g. jammers, intrusion and eavesdropping transmission) for critical satellite datalinks, improving signals protection and integrity.
- Providing future proof interfaces and complementarity to upcoming disruptive security technologies such as quantum, self-healing networks, etc.
- Be open towards upcoming and existing EU-based pooling and sharing programs (e.g. GovSatCom) and satellite constellations (EU Secure Space Connectivity System initiative that is under study) and ready to be integrated in these concepts.

• ***Baseband equipment requirements (hubs, modems):***

- The right implementation of the terminal will determine the success of the EPW. The flexibility and the affordability of the terminal are key considerations. Hence, a Software Defined Mode type of baseband equipment should be pursued;
- The baseband infrastructure (hubs and modems) needs to cover multiple architecture types of networks (point-to-point, point-to-multipoint, mesh) and satellite (wideband, spot beam, mix of both, transparent, processed) architectures;
- The EPW should operate on Software Defined hardware from different vendors that will be selected by nations, government and defence agencies or institutions, depending on their preference or acquisition processes;
- The EPW should include the ability to receive and transmit various modulation methods using a common set of hardware.
- The EPW should be future-proof, easy to upgrade and change configurations (over- the-air) – the ability to alter functionality by downloading and running new software at will, in order to repurpose the modem for a new application;
- The EPW should be affordable and include the latest efficiency satellite waveform, networking and equipment technologies to save OPEX (reduce bandwidth costs, save resources for planning) and CAPEX (save on equipment cost) compared to existing expensive military satellite modems;
- The EPW should consider Size, Weight and Power (SWaP) constraints for on-the-pause and on-the-move platforms and unmanned systems. Modems and terminals should be easy to transport and deployed and use a minimum amount of power;
- The EPW should be deployable in different environment conditions and on different platforms (land, sea or air);
- The EPW should be available in different form factors (OEM cards, rack units or rugged terminals);
- The EPW should be transparent for national encryption standards and externally encrypted data, and capable of integrating on-board modules for encryption technology;
- The EPW should be resilient and maximize service availability to ensure continuity of seamless operations;
- The EPW should have performances considering the throughput demands of today and the future;
- The EPW should support pooling and sharing service models of both waveform and equipment that can be implemented for different operations.
- The EPW should take into account the new use cases and technologies linked to 5G, Machine-to-Machine (M2M), Internet-of-Things (IoT), orchestration, cloud-services, the connected soldier and smart defence.

Expected impact

- Availability of a critical enabler for EU Member States defence forces and CSDP operations and missions in providing scalable secure and resilient communications with protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping;
- Full interoperability between different demanders and suppliers of satellite communication in support of military operations and missions;
- Secure, guaranteed and affordable access to satellite communications for all Member States and CSDP missions and operation;

- Strongly increased European autonomy in satellite communication for defence users and no longer dependency on support from outside the EU for the transmission and exchange of mission critical and sensitive information;
- State-of-the-art technological solution in line with the latest satellite innovations and initiatives such as 5G, broadband connectivity, small LEO/MEO satellites, connected vehicles and Internet of Things.
- Scalable towards existing and planned EU-based pooling and sharing programs (e.g. GovSatCom) and satellite constellations (EU Secure Space Connectivity System initiative that is under study) and ready to be integrated in these concepts.