European
Global Navigation
Satellite Systems
Agency

Clarification Note #1

Procurement procedure: GSA/OP/23/16 – "Development, Supply and Testing of a Galileo Open Service Authentication User Terminal (OS-NMA) for the GSA"

Question no. 1: The contract says that B-IPR should constitute a minor "element" of the "Results" or outputs of the project and that it should be replaceable with an equivalent element without any cost to the GSA. This forces tenderers to conclude that they cannot use any B-IPR if all of tenderer's B-IPR are commercially valuable and not easy to replace with or without the constraint of zero cost to the agency. It would be good to understand the GSA's point of view on this front.

Answer: The draft Contract does not include these limitations. The relevant provisions are recalled and explained as follows.

According to Article I.10.3, the European Union owns the Results and acquires exclusive rights and modes of exploitation.

However, where Background IPR is inserted in the Results, the contracting authority may accept reasonable restrictions impacting on the exclusive rights listed thereto, subject to certain requirements. Namely, that the materials be (i) easily identifiable, (ii) separable from the rest, (iii) do not correspond to substantial elements of the Results, and, (iv)should the need arise, satisfactory replacement solutions exist at no additional costs to contracting authority.

These requirements apply only in case the exclusive rights on the Results are impacted by the Background IPR inserted in the Results.

Question no. 2: Which kind of spoofing scenarios have to be analysed and assessed in the scope of the project? Position only without time drift, or time shift for precise time spoofing?

Answer: The contractor is responsible for identifying and defining the spoofing threats' scenario. A preliminary list of threats shall already be provided in the tender, while the complete set will be defined during the project execution, as per *Sub-task 2.1: Threats identification* of the Tender Specifications.

In terms of anti-spoofing capability to be implemented, as defined in section 2.2.1 of the Tender Specifications, the Contract Stage 1 aims at implementing at least OS-NMA (both at data level and signal level, in accordance with Tender Specifications [AD.1]), while Contract Stage 2 aims at reaching the highest level of robustness by means of a set of additional anti-spoofing techniques which are detailed in section 2.2.7.2.

As outlined in section 2.2.6.2.1 of the Tender Specifications, time synchronisation is also needed for time-delayed key asymmetric protocols as TESLA, which is used for OS-NMA. Consequently, time spoofing can be considered as particularly relevant.

Question no. 3: Why is the tachograph the only application addressed?

Answer: Even though OS-NMA is a capability which can bring added value to many applications, the Smart Tachograph has been identified as an early adopter of the OS authentication.

Question no. 4: Are anti-spoofing techniques involving tight signal monitoring or coupling with other sensors expected?

Answer: As outlined in the Tender Specifications (ref. section 2.2.1 and IMPORTANT NOTE in section 2.2.7.2, among others) the set of anti-spoofing techniques proposed shall also make use of external data from sensors available in the vehicle which can contribute to achieve PVT authentication (e.g. odometer, motion sensors, independent time reference, etc. - see the 'Requirements for construction, testing, installation, and inspection' in Regulation (EU) 2016/799).

Question no. 5: Has OS E1 Anti-Spoofing to be only tackled? What about other frequencies?

Answer: OS-NMA data will be provided in spare bits of the Galileo OS E1B signal, although the authenticated data shall cover both mono-frequency (E1) and dual-frequency users (E1/E5), based on the specification in [AD.1]. Anti-Spoofing techniques shall therefore provide protection to the frequencies used by the User Terminal up to the maximum extent.

Question no. 6: Is a residual vulnerability analysis expected?

Answer: In the scope of task 3 of Stage 1 – "OS-NMA UT v.1 Testing campaign", the contractor shall produce a test report identifying "the weaknesses of the OS-NMA UT v.1 to determine the additional measures to be implemented in stage 2 aiming at achieving the best possible level of confidence of the PVT solution".

In the scope of Contract Stage 2 we expect the contractor to protect against all the pre-identified threats scenarios, therefore no residual vulnerability is strictly foreseen. Should any residual vulnerability still exist, the contractor shall report it into the final report D5-1 OS-NMA UT v.2 Performance Validation Report.

Question no. 7: Is there a maximum delay between the end of Contract Stage 1 and the beginning of Contract Stage 2?

Answer: The maximum duration of the CSPC is 36 (thirty-six) months. The expected duration of execution of the tasks under Contract Stage 1 is 9 (nine) months; the expected duration of execution of the tasks under Contract Stage 2 is 11 (eleven) months.

Thus, provided that the kick off meeting for Contract Stage 1 takes place immediately after entry into force of the CSPC, the maximum delay between the end of Contract Stage 1 and the beginning of Contract Stage 2 would be 16 (sixteen) months.

Question no. 8: Real test using true Signal-In-Space: is there any guarantee related to the availability of OS NMA / public key management?

Answer: The current programme planning foresees a Signal in Space including OS-NMA transmitted from 2018 and the GSA, together with EC and ESA, is working to ensure that. The GSA will provide a schedule at the Kick-Off meeting and inform the contractor about changes during the implementation of the project.

However, due to the importance of testing the UT by means of real SIS, the availability of the SIS containing OS-NMA has been formally set as a pre-condition to activate Contract Stage 2.

The public key shall be provided by the Galileo Service Centre (GSC), either through web portal or via email. The option to distribute the public key through Signal-In-Space shall be confirmed at the project kick-off.

Question no. 9: Are the spoofing scenarios already defined, or shall they be part of the "exhaustive testing" definition?

Answer: The contractor is responsible for identifying and defining the spoofing threats' scenario. A preliminary list of threats shall already be provided in the tender, while the complete set shall be defined during the project execution, as per *Sub-task 2.1: Threats identification* of the Tender Specifications. Based on the full list of identified threats, the contractor shall define the spoofing scenarios to be generated to perform exhaustive testing.

Question no. 10: Are the jamming / spoofing attack scenarios (generally linked) part of the analysis? Should the robustness topic involve the both topics?

Answer: The tender objective is to develop anti-spoofing capability, while anti-jamming is not in the scope as pure jamming cannot be tackled by OS-NMA capability. However, if jamming attacks are perceived as threats complementary to spoofing attacks, the tenderer is invited to propose it for analysis, development and testing.

Question no. 11: Is there a need for support and maintenance for the delivered prototypes? If so, over what period?

Answer: Maintenance is expected for the duration of the contract and the execution of the testing activities to keep the user terminal fully operational and reach the tender objectives. No further maintenance is requested afterwards.

Engineering support is also foreseen along the implementation of the project (see tasks 7.1 and 7.2 of the Tender Specifications).

Question no. 12: How many NMA-enabled satellites need to be operational in order for Contract Stage 2 to proceed?

Answer: Once the OS-NMA data generation capability is implemented in the Galileo Service Centre (GSC) all the operational satellites will be providing OS-NMA data, while they are connected to an uplink station. There is not a minimum number of NMA-enabled satellites to start Contract Stage 2; the precondition is the implementation of the OS-NMA capability within the Galileo system.

Question no. 13: What is required in terms of stamp? How can we get it in UK?

Answer: This question is not clear to us. Please re-submit the question.

Question no. 14: Could the purpose of the Galileo OS-NMA call cover additional fields of application other than the automotive case? Especially, starting from Tachograph for automotive could we derive some feedbacks for position authentication in the field of AUV, train, etc.?

Answer: Smart Tachograph is the target application for the procurement. The analysis of whether the achieved results can be also applicable in other fields of application is not strictly prohibited as long as the tender objectives are met.

Question no. 15: Is the authentication implementation limited to the application of the Galileo OS-NMA only, or other concurrent techniques based on the Galileo PRS service (e.g. remote authentication) could be traded-off?

Answer: The authentication scheme to be implemented in the scope of the current procurement is the one defined in the Tender Specifications [AD.1].

Question no. 17: Is it foreseen to derive some recommendation for other applications such as Avionics & AUV or others (e.g. identification, geofencing, etc.)?

Answer: Please refer to the answer to question no. 14.

Questions received at the webinar of 29 March 2017 which are not answered here will be answered in a forthcoming clarification note.

End of Document