Request for Information (RFI) - Soldier Node.

The Swedish Defence Materiel Administration (FMV) has a need to, on behalf of the Swedish Armed Forces (SwAF), procure equipment for protection and routing of voice and data generated by individual soldiers. The main application for this equipment is to provide individual soldiers in a tactical environment with protection of transmitted voice and data up to and including the classification level Restricted.\(^1\)

FMV needs to explore the market for this type of products. With this Request For Information (RFI) we invite potential suppliers of this kind of equipment to submit information describing their capabilities and products. The information should include a description of the suggested equipment and price information. To aid the suppliers, a simple questionnaire is included with areas where FMV has identified critical technical or regulatory requirements.

This is not a procurement. This RFI does not represent a contract, a promise to contract or a commitment of any kind on the part of FMV.

It should be noted that the purpose is to gather information on what the market has to offer and is not intended as a basis for a quotation from a supplier. FMV will not pay for the received information or cover any costs for any demonstrations of the equipment.

Information requests

While some of the questions read as requirements, FMV stresses that this is not a technical specification in procurement. Thus, while a "fulfilled"/"not fulfilled" answer may suffice for some of them, they really are information requests rather than technical requirements and should be treated as such. Additional comments and argumentation pointing at e.g. technical challenges or cost drivers are appreciated.

The MoSCoW Method of prioritising is used in describing requirements. Requirements in this RFI are based on stakeholder interviews, use case workshops and objectives presented by SwAF.

- **M - MUST:** Describes a requirement that must be satisfied in the final solution for the solution to be considered a success.

- **S - SHOULD:** Represents a high-priority item that should be included in the solution if it is possible. This is often a critical requirement but one which can be satisfied in other ways if strictly necessary.

\(^1\) According to Swedish law "Offentlighets- och sekretesslagen (2009:400, kap 15)" concerning national security.
C - COULD: Describes a requirement, which is considered desirable but not necessary. This will be included if time and resources permit.

W - WONT: Represents a requirement that stakeholders have agreed will not be implemented in a given release, but may be considered for the future.

We have also supplied a number of requirements classified as QUESTIONS where we would appreciate potential supplier’s response to give FMV estimates for future planning.

FMV does not expect any presentation at this stage; however FMV may be interested in an oral presentation or demonstration at a later stage of the assessment process. Furthermore, as part of the response, FMV requests relevant marketing information, product leaflets, system descriptions et cetera, preferably with text and pictures.

Sensitive Information

For legal protection of commercially sensitive data of a participating Company, it is required in accordance with the Swedish Publicity and Secrecy Act (SFS2009:400), that the submitted data contains business or service information/conditions and that there is a specific reason to presume that the Company will suffer damages if the data is disclosed which exceeds the public interest. Therefore, if you as responding Company to this RFI consider that parts of data submitted to FMV fulfil the above referred requirements for secrecy, please mark the specific parts and specify the reasons for the request for commercial secrecy including the damage your Company will suffer if the data is disclosed.
Overview of Soldier Node

Function

The Soldier Node system, also known as “Buret Krypto” in Swedish, shall provide individual soldiers with the ability to encrypt/decrypt voice and data in a tactical environment. It shall also act as a simple communications router connecting the following external devices:

- Headset (clear text audio in, analogue)
- Data in (clear text data IPv4/IPv6)
- Radio 1 (encrypted data, digital)
- Radio 2 (encrypted data, digital)
- Radio 3 ( Clear text audio out, analogue)
- Military Vehicle Intercom/LAN, (digital, VoIP/IP)

The Soldier node shall allow the soldier to simultaneously decrypt and listen to all incoming voice channels and encrypt/decrypt data to be sent to a connected soldier computer. Using an internal and/or wireless external PIT-selector (Push To Talk) the soldier shall choose the routing of voice from the headset to the recipient group. To facilitate handling of the Soldier Node in an uncontrolled environment all personal settings, configuration data and crypto keys shall be stored on a personal “ignition key” device. This ignition key shall be part of the system. Software for preparing configurations and perform administration of the Soldier Node shall also be included in the system.

Figure 1. Soldier Node system with system boundary marked by dotted line.
Operational Context

The Soldier Node has to support a number of different scenarios; a few are given in this part to visualize expected properties.

Basic Soldier

The soldier is equipped with a handheld personal radio (e.g. Harris RF-7800S connected as radio 1 in figure 1), Soldier Node, LS3 (a personal Battle Management System), GPS (Global Positioning System) and headset (e.g. Peltor ComTac XP). Information in voice communications, position and data from LS3 are considered as classified at the level Restricted.

- The soldier has to speak with/listen to other team members
- The soldier has to listen to commands given by group/squad leader.
- Position information and other data has to be exchanged between team members

Variation 1: The soldier could be equipped with an additional radio (radio clear text analogue in figure 1), used for unclassified voice only, to allow monitoring of civilian radio communications. If the soldier has to talk using this radio a warning tone in the headset should make the soldier aware that an unclassified transmission channel is used.

Variation 2: The soldier is travelling in a vehicle where communication is routed from the Soldier node through the vehicle intercom system. The vehicle intercom system in the vehicle handles routing of the encrypted voice and data.

Team Leader/Squad Leader

Same as Basic Soldier but with the addition of an additional radio (see radio 2 in figure 1) used for communicating with platoon leader or for long-range communication.

Other scenarios

To simplify use of the Soldier Node in uncontrolled environment classified information should not remain in the unit when not under direct supervision by the soldier. When replacing units with spares a simple way of moving personal settings, address, configurations and keys to the replacement device is required. The Ignition Key device is expected to be a possible solution in these scenarios.

Scenario 1: The Soldier Node Main Unit belonging to the Team Leader/Squad leader stops working. He decides to shift a functioning Main Unit from one if his team soldiers to himself. By inserting his personal Ignition Key device in the Main Unit from his team member his personal settings should be possible to transfer with minimum effort.

Scenario 2: A Soldier returns to camp/depot/hotel and has to leave his equipment. By removing the Ignition Key device the remaining Main Unit should not contain classified information requiring secure storage.

Requirements

General

Req 1 SHOULD be based on standardized technology.
Comment: Standards such as Suite B cryptography, NATO standards (STANAG) and Internet Standards (RFC) should be used where possible.

Req 2 MUST be approved by Swedish NCSA (National Communications Security Agency) as a COMSEC (Communications Security) device for the Swedish classification level H/R (Restricted).
Main Unit

Req 3  MUST be mounted on the Swedish Vest System used by soldiers.

Req 4  MUST have a maximum weight of 500 grams including battery.

Req 5  SHOULD have a maximum weight of 300 grams including battery.

Req 6  MUST operate a minimum of 16 hours on internal batteries.
   Comment: Given that transmitted data is voice with lower bandwidth than 64 kbit/s and a ratio transmit/receive/standby of 3/6/1.

Req 7  MUST have a minimum data throughput of 2 Mbit/s.

Req 8  MUST be possible to use external power from vehicle (28 V DC).
   Comment: If a rechargeable battery/accumulator is used this should be charged when the main unit is connected to external power.

Req 9  MUST withstand all climatic environments, tropical to arctic (except extreme arctic conditions).
   Comment: All parts of the system mounted on, or used by soldiers in the field, have to withstand climates as per STANAG 4370, AECTP 230 except climate zone C3 and C4. They should also withstand exposure to salt water and petrol based products.

Req 10 MUST have a red/black separation.

Req 11 SHOULD have design separating security and non-security domains.
   Comment: Field upgrades of non-security software such as interface drivers should be possible while still maintaining the integrity of the secure portion, crypto and key management, of the design.

Req 12 MUST be possible to perform field upgrade of non-security related software.

Req 13 MUST support use of multiple crypto keys.

Req 14 MUST allow for separation of different logical channels.
   Comment: As an example this could provide separation of data and voice using different keys or algorithm implementations. Processing (decryption/encryption) on multiple duplex digital data channels is expected.

Req 15 SHOULD have a crypto based on AES (Suite B).
   Comment: Standardized crypto techniques should be used if possible.

Req 16 COULD have support for VPN (Virtual Packet Network).
   Comment: Forming tunnels at OSI-level 2 (Ethernet) and/or 3 (IP).

Req 17 MUST be possible to perform an emergency erase of keys and other classified information without external power.

Req 18 MUST support multicast/broadcast communication.
   Comment: Communication of both data and digitized voice between soldiers in a team/squad is expected to be of this type in a battle field environment.
Req 19  SHOULD support unicast voice communication.
Comment: Establishing a unicast connection should take less than five (5) seconds. In this environment SwAF are fielding other equipment using VoIP (Voice over Internet Protocol) using SIP (Session Initiating Protocol). The Soldier Node should be integrated in this context.

Req 20  MUST be possible to use on board Swedish naval vessels such as Combat Boat 90 (Strb90).

Req 21  COULD be certified for use on board C-17 Globemaster used for troop transport.

Req 22  COULD be certified for use on board helicopters.
Comment: Certification primarily for troop transport helicopters such as NH90 TTH (HKP14).

Req 23  MUST be possible to communicate within 30 seconds after power on.
Comment: The requirement assumes that necessary keys and software are present in the unit.

Req 24  MUST have a display to show status and control feedback.

Req 25  MUST have keys/buttons to allow control and operation.
Comment: Volume Control for headset, controls for keying (PTT) radios and intercom, menu navigation, etcetera.

Req 26  COULD have a numerical Key Pad to allow preparing short (encrypted) messages, enter call signs or other information.

Req 27  MUST support the handheld radio RA 1570 (Harris RF-7800S) and the radio RA1512 (Harris RF-5800H-MP).

Req 28  MUST support STANAG 4591 MELPe Vocoder (1200/2400 b/s).

Req 29  MUST support future soldier radio systems.
Comment: The Soldier Node is expected to have an expected life longer than the radio systems it shall connect to. This means that standardization and possibility to upgrade interface software is essential.

Req 30  WON'T support the radio RA180.
Comment: This radio is not expected to be available in the same military environment as the Soldier Node.

Req 31  MUST support typical circumstances in tactical communications such as long total transmission delay and variation in transmission delay during communication.
Comment: Worst-case scenarios contain technologies such as satellite links, HF radio, and ad hoc routing in radio networks.

**Ignition Key**

Req 32  MUST be possible to carry in a strap around the neck at all times.
Comment: expected to be not larger than a modern car key. Capable of withstanding wet, humid conditions such as showering and sauna.
Wireless PTT (Push-To-Talk) Unit

Req 33 MUST have a Wireless PTT unit with similar function as PTT on main unit.

Req 34 MUST be possible to temporarily mount Wireless PTT in different ways on weapons, steering wheels, handle bars and soldiers wrist.

Administration Software

Req 35 MUST run on standard laptop computer.

Req 36 MUST be possible to configure routing on the Main Unit.
Comment: Scenarios could include re-routing between two radio interfaces without decrypting data based on QoS-information or preventing routing of high-bandwidth data to radio with low bandwidth.

Req 37 SHOULD be possible to program multiple devices connected to a network.

Auxiliary Equipment (Cables, pockets, pouches)

Req 38 SHOULD re-use existing equipment if already available in the Swedish Armed Forces.
Comment: E.g. equipment that is part of, or interfaces the SKE Interface Box (M1892-768011) should be used if possible.

Documentation

Req 39 MUST include documentation for users, service personnel and others.

Req 40 MUST have computer based training software for training of users.

Req 41 MUST be possible to deliver all design documentation (drawings, source code etc.) describing the Soldier Node to FMV and Swedish NCSA (National Communications Security Agency).
Comment: This is a requirement to allow for security reviews by the Swedish authorities before an approval of the crypto can be made.

Commercial Questions

Development phase

The Swedish Armed Forces expect to equip the first military units with the new Soldier Node in mid 2016. During the time period up to this point a development phase, possibly including both validation of functions together with adjoining systems and user experience tests have to performed. These tests will probably be mainly laboratory tests on equipment that at this stage could non-compliant with size, power, weight and environment requirements for the final product. A possible scenario for the development phase could be:

- Project start and System Requirements Review – mid 2012
- First Prototypes - early 2014
- Series delivery and training of first users - early 2016
Series delivery

The Soldier Node will be gradually introduced in the Swedish Armed Forces. Manufacture and delivery is expected to be at a rate to be defined at a later stage. The total number of units estimated cannot be disclosed at this point. When answering the questions below a hypothesis of delivery at the rate given in each requirement below during five years should be used. To give support for planning a number of questions could give us planning background.

Maintenance

The Soldier Node, with a technical life expectancy of ten years, is expected to be used by the Swedish Armed forces for a long period of time. Changes in the Swedish Armed Forces will change the ratio between storage and use of equipment. We expect that equipment will be used more frequently in training and actual field use compared with the previous situation when Sweden had a draft army. We also believe that maintenance will include delivery of software upgrade packages at a rate of 1-2 times each year. Major software upgrades adding functionality are expected at a rate of once every 2-3 years.
Language
All documentation in this procurement matter including all correspondence shall be in the Swedish or English language.

Submission of answer
Answer shall be in FMV possession not later than 2012-06-19.

The answer shall be signed by the supplier and submitted in writing.

An answer that is submitted by telefax or e-mail shall be complete and shall be confirmed immediately by the complete original answer.

The answer shall be addressed to:

Försvarsmaterielverk
Inköpadministrationen
SE-115 88 STOCKHOLM
Sweden

Telefax: +46 (0)8 661 8220

e-mail: eva.hammarlund at fmv.se, with copy to christer.afzelius at fmv.se

Information regarding the RFI
Questions regarding this RFI shall be submitted in writing and shall be addressed to:

FMV
AK Led Inköp
SE-115 88 STOCKHOLM
Sweden

Telefax: 08 - 661 8220

E-mail: eva.hammarlund at fmv.se with copy to christer.afzelius at fmv.se

Contact for technical questions: Christer Afzelius

Contact for commercial questions: Eva Hammarlund

Questions will be received until 2012-06-05. Relevant answers will be distributed on FMV's web site under reference no. 367742. Updates will be published regularly however not after 2012-06-12
All questions and associated responses will be made available on FMV web site without the identity of the person submitting the question or the company identity being revealed.

FÖRSVARETS MATERIELVERK

Peter Schedin                     Eva Hammarlund