Additional information about the Soldier Node

This document contains the RFI for the Soldier Node and the Questions & Answers document for the RFI for the Soldier Node. No additional information is added. Note that this is just information to give a more detailed picture of the Soldier Node.

Documents
- Q_A

Peter Ryner, Project Manager, Ak Led/ Radio
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.

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

\textbf{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 etcetera, 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 PTT-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.

![Diagram of Soldier Node 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 one handheld personal radio (e.g. Harris RF-7800S connected as radio 1 in figure 1), Soldier Node, L53 (a personal Battle Management System), GPS (Global Positioning System) and headset (e.g. Peltor ComTac XP). Information in voice communications, position and data from L5 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 spaces 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 of 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 SwAP 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 (HKP 14).

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
QUESTION: What is an estimated cost for development with a scenario as described?
Comment: We expect a rough order of magnitude estimate (±50%), this figure will be used for FMV internal planning purposes only.

QUESTION: Are there any export restrictions?
Comment: If this is the case please also give an estimate of the time required to get necessary permits.

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.

QUESTION: What is the estimated cost per unit given yearly deliveries of 1 000 units including all auxiliary equipment?

QUESTION: What is the estimated cost per unit given yearly deliveries of 3 000 units including all auxiliary equipment?

QUESTION: What is the estimated cost per unit given yearly deliveries of 5 000 units including all auxiliary equipment?

QUESTION: What is the estimated cost per unit given yearly deliveries of 10 000 units including all auxiliary equipment?

QUESTION: What is suggested to be the preferred batch sizes in the questions above?

Maintainance
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.

QUESTION: What is the estimated yearly cost of maintaining the Soldier Node system?
Comment: This may divided in two parts: fixed and variable cost. A rough order of magnitude estimate is expected.
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:

Försvarets materielverk
Inköpsadministrationen
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
**Question:** Harris radios have their own encryption; the "Soldier Node" shall also provide encryption. Is FMV willing to use the encryption capabilities provided by both the Radio and the "Soldier Node"?

**Answer:** The purpose of the Soldier Node is to provide COMSEC (COMmunications SECurity) for both data and voice generated/received by the soldier. If the radio, as is the case with e.g. some Harris radios, has a built in crypto this will not be relied on for security (COMSEC). In radios where the COMSEC cannot be disabled it will execute but not be used as trusted encryption. The radio crypto will however still provide TRANSEC (TRANsmission SECurity).

**Question:** May you confirm that the separation between red/black is applicable to voice only?

**Answer:** No, the red/black separation shall include both voice and data. It is expected that voice would be digitized in the main unit using a codec such as MELPe before encryption. Data from the Soldier BMS (Battle Management System) shall also be encrypted by Soldier Node before being transmitted. The data from the BMS to be encrypted is expected to be IPv4/IPv6.

**Question:** May you confirm that no cross-domain security data gateway is necessary for the described solution since the "Unclassified radio" is only voice capable?

**Answer:** Yes, that is correct. To avoid unintentional data leakage there is a simple design rule for the black side of Soldier Node: All encrypted information (data and voice) shall only be available at the digital interfaces (Radio 1/Radio 2/Vehicle Intecom) and clear voice (uncrypted) shall only be available on the analogue interface connecting the "Unclassified Radio". The connection to the “Unclassified Radio” should be seen as a pass through/replication of the headset connection. There can be no routing/retransmission of voice between radios connected using an analogue and a digital interface.

The following questions were in Swedish and have been translated by FMV. The original text is in italics.

**Question:** In Req 6 - What is meant by ratio for transmit/receive/standby of 3/6/1? *(Vad menas med ratio for transmit/receive/standby of 3/6/1?)*

**Answer:** The ratio describes relative relations between the time the main unit is used for different tasks. The relations are between encryption of data (30% of the time), decryption (60%) and standby/idle (10%) of the total time in use. We are aware that this measure is simplified when multiple encryption/decryption task may be performed simultaneously. It shall be seen as an indication on the traffic load only on the radio interfaces.

**Question:** In Req 10 – It is stated that the product must have a red/black separation. The product in question must meet the Swedish classification level H/R (Restricted). In the Swedish regulatory guide "HTST-Grunder" a red/black separation is required for the level H/S (Secret) but is not mentioned for the level H/R (Restricted). Could you please clarify to what degree a red/black separation is expected. Does this mean that the device has a red and a black interface, that there is an interior module (crypto module) with a red and a black interface or that there is a defined red/black separation in this module. Or do you mean something else by this? *(Den produkt som frågas efter skall klara signalkyldssgrad H/R. I HTST-Grunder nämns inte rödsvart separering i samband med H/R men däremot i samband med H/S. Skulle ni vilja förtydliga på vilken nivå rödsvart separering förväntas. Betyder det att apparaten har ett rött och ett svart interface, att det finns en inre modul (krypto modul)*
som har ett rött och ett svart interface eller att i kryptomodulen finns en definierad rödsvart separation i hårdvara. Eller är det något annat som avses.)

**Answer:** The intention is to have three well defined zones in the Main Unit: Black, Red and “Crypto”. It is expected that red and black zones contain software that may be reprogrammed/upgraded/exchanged fairly often whereas the crypto zone would be fairly static (difficult to change). A purely logic red/black separation could be possible according to regulations but proximity to radio equipment does however make requirements for a more strict red/black separation probable.

**Question:** Provided the Project start and System Requirements Review are planned for mid 2013,

**Answer:** Our preliminary plan is that an RFP/RFQ will be posted Q1/Q2 2013.

**Question:** Shall it be possible to operate audio services when only the Soldier Node and one (or more) radio is present, i.e. in the absence of the Soldier BMS?

**Answer:** Yes, in many cases a minimum configuration with headset, Soldier Node and one single radio is to be expected. This configuration would provide the soldier with secure audio services.

*The following questions were in Swedish and have been translated by FMV. The original text is in italics.*

**Question:** Is there a better system picture of typical use, which you can share? (*Finns bättre systembild över typisk användning att delge?*)

**Answer:** No. Work is on-going and FMV are still in the process of developing detailed use cases.

**Question:** Interface "Data In" on page 3, we assume this is Ethernet. Are there any requirements on using optical or electrical interface? Is this always a plain text interface, or are occasions where the encrypted data shall be routed to the next radio system through this interface (Req 36)? (*Interface ”Data in” på sid 3 antar vi är Ethernet. Finns krav på optiskt eller kan elektriskt gränssnitt användas? Alltid ett klartext interface eller finns tillfällen där krypterad data ska routas vidare till nästa radiosystem via detta gränssnitt (Req 36)?*)

**Answer:** FMV are presently working on the Interface Specifications for the Main Unit. The assumption at this point is that the interface in question is electrical Ethernet. All data on this interface is expected to be valid IP messages. The Main Unit cannot distinguish if these messages are encrypted by other crypto systems in series with the Main Unit.

**Question:** Interface "Military Vehicle Intercom / LAN" on page 3, we assume that this is also Ethernet. Are there any requirements on using optical or electrical interface? Is it always a ciphertext interface or are occasions where the plain language voice / data to be handled in any type of vehicle?

(*Interface ”Military Vehicle Intercom/LAN” på sid 3 antar vi också är Ethernet. Finns krav på optiskt eller kan elektriskt gränssnitt användas? Alltid ett kryptotext interface eller finns tillfällen där klartext tal/data ska hanteras i någon fordonstyp?*)

**Answer:** FMV are presently working on the Interface Specifications for the Main Unit. The assumption at this point is that the interface in question is electrical Ethernet. All user data exiting this interface will be encrypted.
**Question:** Interface descriptions for radio systems 1-2 would be desirable. Which electrical interfaces required at Soldier Node to respond to current and future radio systems? (Gränssnittsbeskrivningar för radiosystemen 1-2 vore önskvärt. Vilka elektriska gränssnitt behövs på Soldier Node för att svara upp mot nuvarande och framtida radiosystem?)

**Answer:** It is expected that the interface for radio systems 1-2 would be Ethernet/IP for future radio systems. Solutions to provide support for the Harris radios mentioned are necessary even though interfaces in these radios are not IP. FMV is at this time unable to give out detailed interface descriptions for the current radio systems due to commercial agreements.

**Question:** (Req 2) How will the Swedish TEMPEST (RÖS) requirements for the level Restricted be interpreted for Soldier Node? (Hur kommer de svenska RÖS-kraven för HI/R tolkas för Soldier Node?)

**Answer:** FMV expects that a conservative view will be taken for the TEMPEST (RÖS) requirements as the crypto will be in close proximity to radio transmitters. This means that special precautions will be required to avoid unintentional disclosure of classified data.

**Question:** (Req 2) Will evaluation according to Common Criteria (CC) be required and if so, at what level? (Kommer krav på CC-evaluering ställas och i så fall till vilken nivå?)

**Answer:** We do not know at this stage. Even in cases when a formal certification is not called for, the processes in Common Criteria are often used in Swedish crypto development.

**Question:** (Req 2) What are the requirements on separation of the cryptographic function? Does the Swedish NCSA (MUST) expect it to be implemented in separate processor / hardware? (Vilka krav gäller på separation av kryptofunktionen? Förväntar sig MUST att den implementeras i separat processorn/härvar?)

**Answer:** Based on discussions with Swedish NCSA (MUST) during the system definition phase, FMV expects that the cryptographic function must be clearly defined and well separated from other communications processes.

**Question:** (Req.10) Vilka typer av röd/svart-separation kommer MUST anse uppfyller kravet?

**Answer:** We do not know at this stage.

**Question:** (Req.11) What are the various separate information domains predicted? What threats are foreseen for different interfaces? Req 36 and 37 indicate network connection via Ethernet and TCP / IP on both the red as the black side of Soldier Node in the system image. Does this require protection against full-scale cyber attacks on the interface or can any of the networks be considered safe? (Vilka olika separerade informationsområden förutses? Vilka hot förutses för olika interfacet? Req 36 och 37 antyder nätverkskoppling via Ethernet och TCP/IP på såväl röd som svart sida av Soldier Node i tänkt systembild. Innehårb detta krav på fullskalig skydd mot olika IT-attacker för dessa interfacet eller kan något av nätten anses säkra?)

**Answer:** The domains we expect are red user data (voice and data), crypto domain including key management and black data. Basic security measures are expected on the interfaces. The red interface is considered to be somewhat more secure as it is under user supervision. Our analysis of threats is classified and will not be made available at this stage.

**Question:** (Req 26) Will some soldiers not have Battle Management Systems (BMS)? Would it suffice to be able to view text messages for those who do not have BMS?
(Kommer vissa soldater inte ha BMS? Skulle det räcka med att kunna visa texnodedelen för de som inte har BMS?)

**Answer:** Many soldiers will only have a headset, Soldier Node and a radio. The suggested function is seen as a simple way to send text messages between Soldier Nodes without the need for a BMS. There is no requirement at this point that these text messages shall be possible to send from a BMS to the Soldier node.

**Question:** (Req.28) Is there a request for a codec with higher bandwidth for better voice quality when available bandwidth allows it? MELP2400 does not give very high speech quality. (Finns det önskemål om bredbandigare talkodare för bättre talkvalitet när tillgänglig bandbredd tillåter det? MELP2400 ger ju inte så hög talkvalitet.)

**Answer:** The Soldier Node is expected to be used in a tactical environment were bandwidth is very limited. Alternative codecs could be implemented, however always with focus on battlefield requirements.

**Question:** (Req 33) Please describe intended function of the Wireless PTT. Should the user be able to select which radio to use? Should it control a specific radio control to select one of several configured radio channels? How many choices should be possible to make via the device? (Beskriv gärna tänkt funktion på Wireless PTT. Skan man kunna välja vilken radio som ska användas? Skan man kunna styra en specifik radio att välja en av flera konfigurerade radiokanaler? Hur många val ska göras via enheten?)

**Answer:** There may be different ways to design this. In existing equipment used by the Swedish Armed Forces the PTT buttons correspond to a transmission equipment each. In this existing equipment there are three buttons (Radio 1, Radio 2 and LTS (Local Telephony System). However we expect that in the future the push of a button on the PTT could correspond to a pre-planned logic group (based on e.g. IP address). This would then control routing on the black side. In most cases we do not expect the Soldier Node to control the radio channel settings.

**Question:** (Req 36) Referring to a previous question, more system images are desirable. Req 36 indicates that the black information should be routed further. Which interfaces should be used for this? Only between Radio 1 and 2 interfaces? Or via Ethernet and Military Vehicle Intercom / LAN (seems more logical because of the red-black separation) or data set?

(Enligt fråga 1, mer systembilder önskvårt. Req 36 anger att svart information ska routas vidare. Över vilka interface? Endast mellan Radio 1och 2 interface? Eller via Ethernet och Military Vehicle Intercom/LAN (känns mer logiskt på grund av röd-svart-separerings) eller Data in?)

**Answer:** The primary reason for routing black data is to distribute data for the Battle Management System between soldiers in a group. This information should be retransmitted on the black side to all the logical addresses, independent of physical interface, given in the routing tables of the Soldier Node Main Unit.

**Question:** (Req 37) We interpret Req 37 as a PC with administrative software to communicate with several Soldier Nodes that are interconnected in a network. Referring to a previous question, more system images are desirable. Over which interface? Data in (seems more logical) or Military Vehicle Intercom / LAN? (Vi tolkar Req 37 att en PC med administrativ programvara ska kunna kommunicera med flera Soldier Nodes som är sammankopplade i ett nätverk. Enligt fråga 1, mer systembilder önskvårt. Över vilket interface? Data in (känns mest logiskt) eller Military Vehicle Intercom/LAN?)


Answer: Administration is expected to be done with the unit engaged in a separate mode. The interface to be used is red data in.

Question: (Req 38) Desirable with description of SKE Interface Box. What does it do? Which interfaces are supported? (Önskvärt med beskrivning av SKE Interface Box. Vad gör den? Vilka interface stöds?)
Answer: The SKE Interface Box is an interface box similar functions as the Soldier Node. The SKE has a wireless PTT and can control communication from a headset to two radios and a Local Telephone System (LTS). The SKE only handles analogue signals on all interfaces. The requirement for re-use or coordination with the SKE could include using the same type of headset connectors and batteries.

Question: Are there any requirements on the size? (Finns det krav på storleken?)
Answer: No, not at this time.

Question: Is there any requirement that the production of all or part of the equipment shall be made in Sweden? (Finns det några krav på att produktion av hela eller delar av utrustningen ska ske i Sverige?)
Answer: No. The normal processes used for bilateral exchange of classified information are expected to be sufficient.

Question: What is the background to the requirement to use an external crypto and not embedded solutions? (Vad är bakgrunden till att kravställa ett externt krypto och inte inbyggda lösningar?)
Answer: Security approval of each new system is complicated and expensive. By combining an external crypto with additional functionality such as routing we expect to gain more value from a user perspective compared with many different embedded solutions. The use of an external system can also give new abilities not limited by the architecture of the radio network.