SCA COMPLIANT, SUITE B COMPATIBLE MULTIBAND HANDHELD RADIO

Igor A.(Tony) Spivak (Harris Corporation, Rochester, NY; e-mail: ispivak@harris.com)

ABSTRACT

In an effort to create a flexible and adaptable cryptographic strategy, the US Department of Defense announced a set of cryptographic algorithms for protecting both unclassified and certain classified national security information. This set of cryptographic algorithms is referred to as Suite B. The Suite B set is based on the cryptographic algorithms approved by the National Institute of Standards and Technology (NIST), thus it is ideally suited as the base for cryptographic interoperability between products manufactured by different vendors. The Harris Falcon III® RF-310M-HH Suite B Compatible Multiband Handheld Radio is the first Software Communications Architecture (SCA) based tactical military radio product to implement the set of Suite B Cryptographic Algorithms. The RF-310M-HH is presently undergoing US DOD evaluation and once certified will be approved to support secret and below voice and data communications. An additional differentiating advantage offered by this Suite B compatible radio product is that it does not require special handling, accounting controls and markings which are typically associated with Controlled Cryptographic Items (CCI). Hence, the RF-310M-HH Multiband Handheld Radio is a Suite B Compatible, non-CCI, electronic communications product designed for secure communications at secret and below level. This paper describes the Suite B initiative strategy and goals as they apply to both tactical military radio communications and public safety radio communications environments. The paper also describes the Harris Falcon III® RF-310M-HH Suite B Compatible Multiband Handheld Radio product, the market needs this product will address, as well as the consideration of ideas for a future set of capabilities.

1. INTRODUCTION

Radio system interoperability issues have been in the forefront of the news media in recent years. The tragic events of September 11 and Hurricane Katrina highlighted serious problems faced by first responders from different organizations, as they were unable to communicate with each other. The primary reasons for these issues were the mix of operating frequency ranges and incompatible modes utilized by different branches of first responders.

In the realm of tactical military radio communications, the current threats and challenges the US DOD faces are very different from the cold war threats and challenges of the past. Though there is still a need for high grade communications systems that are able to support US only top secret traffic, more and more emphasis is being placed on interoperable systems that are capable of supporting secret and below communications traffic. In Iraq and Afghanistan, the ability to communicate securely between branches of US military and coalition forces is of paramount importance. Today's primary method for secure communications in the theater of operations is by using high grade, Type 1 CCI radio systems; the same systems being used for US only top secret communications traffic. These high grade systems are intended for use by US forces as well as some NATO member countries. There are, however, many other friendly factions, both local and foreign, that need to communicate securely with the US and NATO coalition forces. Due to the lack of interoperable radio systems, the US DOD frequently has to decide between providing high grade, Type 1 CCI radios to those factions or accept the risk of not being able to securely communicate with them. Typically, the need for secure communications outweighs the risk of the radio systems being improperly used or exploited, and the high grade, Type 1 CCI radios are provided.

Many aspects of the communications system design must be considered to ensure end to end interoperability. Some of these aspects include communications waveforms, protocols, modem signaling schemes and cryptography. This paper focuses on the cryptographic aspect of radio system interoperability. As part of the Cryptographic Modernization Program to transform and modernize the Information Assurance capabilities for the 21st century, the US DOD has defined Suite A and Suite B sets of cryptographic algorithms. The Suite A set contains classified, US-only algorithms designed to protect the most sensitive national security related information. The Suite B set contains strong commercial algorithms designed to facilitate cryptographic interoperability.

The Harris Falcon III® RF-310M-HH Suite B compatible Multiband Handheld Radio is the first Software Communications Architecture (SCA) based radio product designed to bridge the interoperability gap based on the Suite B set of algorithms. The RF-310M-HH radio will be certified to process secret and below traffic and will not require CCI handling procedures. The Harris Falcon III® RF-310M-HH Radio is scheduled to be released into production in the summer of 2009.

2. DEPARTMENT OF DEFENSE SUITE B CRYPTOGRAPHIC INTEROPERABILITY INITIATIVE

In 2005, the National Security Agency, recognizing the need for cryptographic interoperability based on a set of strong commercial algorithms, promulgated the Suite B Cryptography [1]. The Suite B set only specifies the cryptographic algorithms. It does not dictate the process or the requirements for the development of Suite B compatible products. Suite B includes the following set of algorithms:

- Encryption/Confidentiality - Advanced Encryption Standard (AES) – specified in FIPS 197 (key sized 128 and 256 bits) [2].

- Digital Signature/Authentication – Elliptic Curve Digital Signature Algorithm (ECDSA) – specified in FIPS 186-3 (using the curves with 256 and 284 bit prime moduli) [3].

- Key Exchange – Elliptic Curve Diffie-Hellman (ECDH) – specified in Draft NIST Special Publication 800-56 (using 256 and 384 bit prime moduli) [4].

- Hashing – Secure Hash Algorithm (SHA) – specified in FIPS 180-2 (using SHA-256 and SHA-384) [5].

Systems that implement ALL of the Suite B cryptographic algorithms are considered to be Suite B compliant. Systems that implement a subset of the Suite B algorithms are deemed Suite B compatible. Not all communication systems require implementation of all of the Suite B algorithms. For instance, tactical multiband radios that support AM/FM voice communications and simple streaming RS-232 synchronous/asynchronous data communications may implement the AES encryption algorithm for user traffic confidentiality. However, the ECDH algorithm may not be implemented in such radios, given the radios' inability to support networking waveforms and lack of wireless or wired connectivity to the required servers and databases.

Implementation of the Suite B cryptography alone is not sufficient to ensure interoperability. Other aspects such as communications waveforms, protocols and modem signaling schemes must be properly specified to ensure end to end interoperability. Frequently, these aspects are specified in broader interoperability standards such as Association of Public Safety Communications Officials Project 25 (APCO P25) [6] and Secure Communications Interoperability Protocol (SCIP) [7].

There are also aspects of the cryptographic algorithm details that can potentially vary between implementations. The National Institute of Standards and Technology (NIST) defines a number of modes in a series of special publications that apply to AES as well as other block cipher modes. Special Publication 800-38A [8] defines five confidentiality modes for block cipher modes as follows:

- Electronic Codebook (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback (CFB) Mode
- Output Feedback (OFB) Mode
- Counter (CTR) Mode

Additionally, more recent publications define new modes that implement additional authentication functions, as follows:

- Cipher-Based Message Authentication Mode (CMAC)
- Counter with Cipher Block Chaining-Message Authentication Code (CCM)
- Galois/Counter Mode (GCM)

These modes are defined in NIST Special Publications 800 – 38B, 800 – 38C and 800 – 38D respectively [9], [10], [11].

Initialization Vector (IV) format and size are other variables that need to be specified to ensure cryptographic interoperability. The initialization vector is a block of bits that prevents repetition of sequences in encrypted text. A pseudo-random number is frequently used as the IV.

Typically, the specifics of the cryptographic algorithm are further refined in a higher level waveform or protocol specification. For example, SCIP uses AES Counter Mode (CTR) for point to multi-point communications. In another

example, RFC3602 – "The AES – CBC Cipher Algorithm and Its Use with IPsec" [12] specifies the type and the size of the Initialization Vector.

3. HARRIS SOFTWARE DEFINED RADIO EXPERIENCE

The Joint Tactical Radio System (JTRS) Program is a key US DOD initiative to transform the legacy military communications systems to modern, technologically advanced, interoperable and upgradable communications systems that will ultimately result in war fighters' informational superiority on the battlefield. A key enabler that allows the JTRS program to achieve its objectives is the Software Communications Architecture (SCA). The SCA is an open architecture framework that defines how elements of the communications system can be designed, implemented and integrated within a specific radio hardware platform. The main advantage of SCA based systems is portability of SW components, such as waveforms, between different radio hardware platforms. The SCA concept is analogous to SW applications written for a specific operating system that are able to execute on multiple different hardware platforms. Radio systems designed to be compliant with SCA are considered Software Defined Radios (SDR).

Harris has a long, successful track record developing software based radio systems. In the late 1980s, the Harris RF-5000 was one of the first radio products that implemented the majority of the radio functions, such as radio control, modems and Digital IF in software. Though not a true SDR, as defined by today's SCA standards, the RF-5000 was a pioneering radio that paved the way for concepts which ultimately resulted in the SCA.

Harris also has a long history of involvement with the JTRS programs of record, as well as development of the commercial SDR solutions [13]. In the early days of the JTRS development, Harris participated in key activities such as Step 1 and Step 2B/2C programs. These programs validated the SCA based JTRS technology as it applies to tactical radio products. Harris Sierra II Based Crypto Sub-System (CS/S) and the associated Cryptographic Equipment Applications (CEAs) comprise the standard programmable cryptographic solution for many JTRS system applications. Presently, Harris is one of the contributors to the JTRS Ground Mobile Radio (GMR) program.

Figure 1 - AN/PRC-152(V)1(C)

Involvement with the JTRS technology from its inception allowed Harris to leverage its experience in the development of SCA based tactical radio products. The Harris AN/PRC-152(V)1(C) Multiband Handheld Radio (Figure 1) is the first SCA JTEL [14] and NSA Type 1 certified tactical handheld radio. The radio operates in the 30 – 512 MHz frequency range and has both 5W and 50W transmit power configurations. The AN/PRC-152(V)1(C) is a dual mode radio, implementing both Suite A and Suite B algorithms. To date, Harris has delivered more than 80,000 AN/PRC-152(V)1(C) Multiband Handheld radios.

The Harris AN/PRC-117G(V)1(C) (Figure 2) is the first SCA JTEL and NSA Type 1 certified tactical wideband networking radio. The AN/PRC-117G(V)1(C) is also a dual mode radio, implementing Suite A and Suite B algorithms. Both radios support a number of key JTRS waveform applications including:

- VHF/UHF LOS (VULOS)
- HAVEQUICK I/II
- SINCGARS ESIP
- Mil-Std-188-181B
- High Performance Waveform (HPW) – SATCOM
- APCO P25 (public safety waveform)
- DAMA

In addition, the AN/PRC-117G(V)1(C) implements the Harris Proprietary Advanced Networking Wideband Waveform (ANW2). The ANW2 is a mobile ad hoc networking waveform that supports seamless, simultaneous, secure voice, data and real time video communications.

Figure 2 - AN/PRC-117G(V)1(C)

As stated above, the AN/PRC-152(V)1(C) and the AN/PRC-117G(V)1(C) are dual mode; they both implement Suite A and Suite B algorithms. Both radios implement AES encryption as an option within the VULOS waveform. As will be shown later, this capability, along with the APCO P25 waveform, is critical to facilitate Suite B based cryptographic interoperability.

4. HARRIS RF-310M-HH SUITE B NON-CCI, SECRET AND BELOW RADIO

During the summer of 2008, Harris held a number of meetings with the NSA to identify the requirements and define the evaluation process for the first Suite B compatible, non-CCI, Secret and below tactical radio product. These activities led to the development of the RF-310M-HH Multiband Tactical Radio (Figure 3). The RF-310M-HH is presently completing final integration and testing and is scheduled to be released into production in the July, 2009 time frame. The RF-310M-HH radio architecture and design are based largely on the AN/PRC-152(V)1(C) multiband handheld radio. The SCA based software programmable nature of the Falcon III radios allowed Harris to reuse most of the HW assemblies and many of the SW components from the AN/PRC-152(V)1(C). At the core of the RF-310M-HH is the Sierra IIB Cryptographic Subsystem (CS/S). The Sierra IIB CS/S implements the required Suite B cryptographic algorithms and provides other INFOSEC related services, such as key management and bypass. The Sierra IIB CS/S SW was separately evaluated and has been certified by the NSA in June, 2009. The Sierra IIB CS/S SW is a stand-along application that's available for porting to other product applications.

The initial release of the RF-310M-HH Suite B Multiband Handheld Radio supports the following waveform applications:

- VHF/UHF LOS (VULOS)
- APCO P25 (public safety waveform)

The Suite B version of the VULOS waveform supports Continuously Variable Slope Delta (CVSD) modulation for secure voice and synchronous/asynchronous RS-232 DTE data using 128 and 256 bit AES encryption. The modem signaling is Harris proprietary and will allow the RF-310M-HH radio to interoperate with the Harris AN/PRC-152(V)1(C) and AN/PRC-117G(V)1(C) radios provided the same AES traffic key is loaded into each of the radios. All of the Harris Falcon III radios, including the RF-310M-HH, support the Electronic Key Management System (EKMS-308 specification) based key fill interface for loading COMSEC traffic keys.

Figure 3 - RF-310M-HH

The APCO P25 waveform is implemented as a Type 3 waveform in the RF-310M-HH radio, thus it is not certified to support classified user traffic. The APCO P25 waveform implements the Improved Multi-Band Excitation (IMBE) vocoder for voice communications. Voice privacy is available using SW based AES encryption engine implementation.

5. INTEROPERABILITY SCENARIOS

There are many scenarios that could serve as real-life examples of usability for this set of interoperable radio products. Two examples that will be considered in this paper are:

- Military Coalition Operation
- Department of Homeland Security (DHS) Mission

5.1. Military Coalition Operation

Modern military conflicts typically involve multinational forces that may include both NATO and non-NATO member countries. These units require interoperable secure communications. Examples of recent missions include infantry platoons from different nations operating together in search operations in Afghan villages and Forward Area Controllers (FACs) requesting support from NATO or US aircraft. Presently, these types of communications are performed using US high grade, Type 1 CCI radios for secure communications or other non-CCI radios running in Plain Text mode when high grade, Type 1 radios are not available. The RF-310M-HH Multiband Radio will allow these multinational forces to communicate securely up to secret level using VULOS voice and DTE data modes. Since the RF-310M-HH radios are not CCI, handling and distribution of these radios are less complicated.

There is another scenario where the RF-310M-HH radio can help facilitate secure communications between US DOD forces that employ the US Type 1 Suite A/Suite B dual mode radios and coalition forces who would employ the Suite B mode of the RF-310M-HH. More than 80,000 AN/PRC-152(V)1(C) Multiband Handheld radios have been delivered since 2003. A large majority of these radios are being actively used in Iraq and Afghanistan by US and NATO military forces. The AN/PRC-117G(V)1(C) Multiband Manpack Radio is a newer product, thus fewer of those radios have been fielded. As stated in Section 3, both the

AN/PRC-152(V)1(C) and the AN/PRC-117G(V)1(C) implement VULOS waveform using AES encryption. This Suite B mode is identical to the VULOS/AES mode implemented in the RF-310M-HH radio. Thus all three radios share a secure interoperable communications mode.

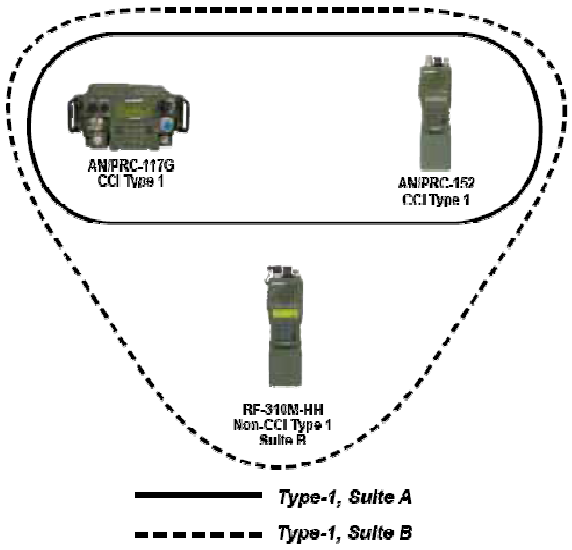

Figure 4 - DOD Interoperability Example

Figure 4 is a pictorial representation of this scenario. The solid oval represents the AN/PRC-152(V)1(C) and the AN/PRC-117G(V)1(C) radios communicating using Type 1 Suite A modes and algorithms such as SINCGARS/VINSON, HPW/KG-84, etc. These types of communications would typically be between US DOD forces or between US DOD and NATO forces with classification levels up to Top Secret. The dashed triangle includes the Type 1, Suite A / Suite B capable radios and also adds the RF-310M-HH Suite B radio. When configured for VULOS/AES Suite B mode, the AN/PRC-117G(V)1(C) and the AN/PRC-152(V)1(C) will interoperate securely with the RF-310M-HH radio. To facilitate this scenario all three radios must be properly configured and keyed. For example, Net 1 can be programmed as the Suite B VULOS/AES coalition net, and Net 2 can be programmed as a SINCGARS/VINSON US only net. The US DOD users would use Net 1 setting to communicate with coalition forces and Net 2 setting to communicate amongst US DOD forces.

5.2. Department of Homeland Security (DHS) Mission

During times of natural or man-made disasters the Department of Homeland Security (DHS) requires secure communications between National Guard, Federal Agencies, State/Local Law Enforcement Agencies and Emergency Services. Much effort is under way to standardize all aspects of DHS communications. APCO P25 is a suite of digital radio communications standards for use by federal, state and local public safety agencies. The APCO P25 standard was established to address the need for common public safety radio communications for first responders and other emergency response professionals. The APCO P25 standard calls out 256 bit AES encryption algorithm, which is the standard Suite B encryption algorithm. The APCO P25 standard also calls out other encryption algorithms, such as 128 bit AES and legacy Data Encryption Standard (DES). The Harris RF-310M-HH radio implements the APCO P25 waveform using the Suite B 256 bit AES encryption algorithm. Since it's not practical to provide high grade, Suite A, CCI radios to law enforcement and emergency response personnel, the RF-310M-HH is an ideal multiband radio product that can facilitate secure, standards based voice communications for first responders and other emergency response professionals. The RF-310M-HH APCO P25 AES implementation is not certified to support classified traffic; however, the Type 3 security implementation of the waveform in the RF-310M-HH radio should be sufficient for most public safety applications.

The Harris dual mode Suite A / Suite B AN/PRC-152(V)1(C) radio also implements the APCO P25 waveform. Thus the RF-310M-HH and the AN/PRC-152(V)1(C) are able to securely interoperate using APCO P25. An example of a relevant scenario can occur when National Guard personnel, who use AN/PRC-152(V)1(C) radios, are required to provide assistance to first responders in emergency situations. Figure 5 shows how APCO P25 secure communications nets could be established using the Harris RF-310M-HH radio, AN/PRC-152(V)1(C) radio and another COTS Land-Mobile Radio which is capable of supporting the APCO P25 waveform.

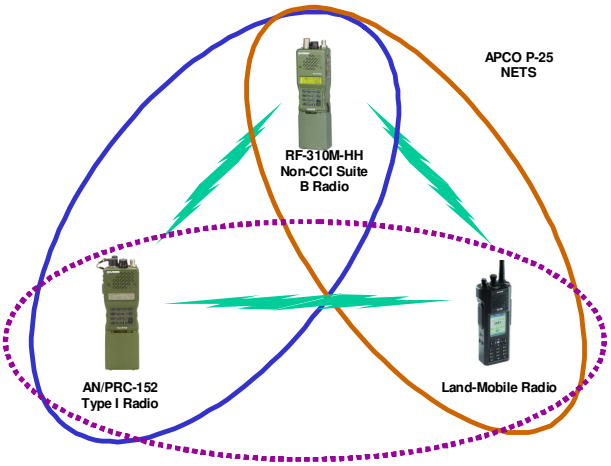

Figure 5 - DHS Interoperability Example

6. FUTURE DEVELOPMENTS

The initial release of the RF-310M-HH Suite B non-CCI Handheld radio will support VULOS/AES secure voice and data modes and APCO P25 secure voice mode. The VULOS waveform implementation will allow the RF-310M-HH to interoperate with other Harris products that implement the VULOS/AES waveform. In order to facilitate interoperability with a broader range of Suite B compatible products including non-Harris products, additional standards based modes must be implemented in the radio.

Secure Communications Interoperability Protocol (SCIP) is a relatively recent application layer interoperability standard that was developed for secure voice and voice band data communications between international coalition partners. SCIP is specified in NATO Standardization Agreement STANAG 5068 [7]. The set of specifications that comprise SCIP has been developed by the SCIP International Interoperability Control Working Group (SCIP IICWG). SCIP specifies AES encryption for confidentiality. SCIP-232 [15] is one of the SCIP specifications that defines the parameters for the AES algorithm. As an active participant in the SCIP IICWG, Harris has generated a proposed specification for SCIP terminals connected via 25 KHz VHF Line of Sight (LOS) Tactical Radio Channels [16]. That specification will likely become one of the SCIP standards and it will ensure that SCIP compliant radio products produced by different vendors can provide end to end secure voice interoperability. Harris intends to implement a SCIP compliant voice mode in a subsequent software release of the RF-310M-HH multiband radio.

Another area of potential new investment in a Suite B compatible radio product would be a Suite B multiband radio dedicated to the Public Safety market and certified for secret and below communications. As stated above, the APCO P25 waveform is implemented as a Type 3 waveform in the RF-310M-HH radio. Though it utilizes the Suite B compatible encryption algorithm for confidentiality, it is not certified to process classified information. There are available radio products, such as Motorola XTS-5000, that support Type 1, Suite A encryption algorithms and are certified to process up to top secret traffic. However, those radio products are CCI and must comply with the associated handling and tracking rules.

The Suite B version of the Harris XG-100 Unity multiband public safety radio would allow classified APCO P25 voice communications up to secret level and would not require CCI handling and tracking. Harris is presently evaluating the market need for this potential new product.

All of the radio products discussed so far have been voice radios with limited (sync/async DTE) data capabilities. Harris presently manufactures a number of radio products that support IP data networking. As stated in Section 3, the AN/PRC-117G(V)1(C) Manpack Radio implements ANW2, which is a networking waveform that supports secure IP data communications. The AN/PRC-117G(V)1(C) implements the High Assurance Internet Protocol Interoperability Encryptor (HAIPE) Specification. Current HAIPE specification only specifies Suite A algorithms for confidentiality and key exchange; however, there is work in progress within the DOD and industry to define the network security specification for Suite B networking products. This Suite B network security specification will call out AES for Encryption/Confidentiality and ECDH for electronic key exchange. Radio products that support Suite B based secure networking will likely be the first products that implement all of the Suite B specified algorithms, thus they will be the first Suite B compliant (as opposed to compatible) products.

7. CONCLUSION

"Take Away Messages"

- Radio systems interoperability is critical in both Military and Public Safety/First Responder communications scenarios. Cryptographic interoperability is an important aspect of the overall

interoperable radio communications system solution.

- Under the Cryptographic Modernization Program, the US Department of Defense defined the set of Suite B cryptographic algorithms to facilitate cryptographic interoperability between communications systems designed and manufactured by different vendors.
- The Harris RF-310M-HH is the first Suite B compatible SCA based software defined multiband handheld radio. The RF-310M-HH will be certified by NSA to support secret and below voice and data communications traffic. The RF-310M-HH radio is not a COMSEC accountable item (non-CCI).
- The RF-310M-HH Suite B multiband radio, along with other Harris dual mode Type 1, Suite A / Suite B radio products can support a number of mission critical communications scenarios, both in the battlefield and in the area of public safety communications.
- Future developments, such as SCIP protocol implementation and networking waveform support, will increase interoperability and usability of Suite B radio products.

8. REFERENCES

[1] NSA Suite B Cryptography Definition, date posted: Jan. 15, 2009, NSA Suite B Cryptography - NSA/CSS,

[2] FIPS PUB 197, Advanced Encryption Standard (AES), November 26, 2001.

[3] FIPS PUB 186-3, Digital Signature Standard (DSS), June 2009.

[4] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, U.S. DoC/NIST, March, 2007.

[5] FIPS PUB 180-2, Secure Hash Standard , August 1, 2002.

[6] APCO Project 25 Statement of Requirements, October 17, 2008.

[7] STANAG 5068, (Edition 1), Secure Communications Interoperability Protocol (SCIP), Working Draft V0.1, 28 August, 2008.

[8] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, U.S. DoC/NIST, December, 2001.

[9] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Authentication Mode. U.S. DoC/NIST, May, 2005.

[10] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality. U.S. DoC/NIST, May, 2004.

[11] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. U.S. DoC/NIST, November, 2007.

[12] Network Working Group Request for Comments (RFC) 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec. September, 2003.

[13] Turner Mark R., “Software Defined Radio Solutions”, SDR Forum ’07, Denver, CO

[14] News Release – Harris Corporation, “Harris Corporations’ Falcon III AN/PRC-152(V)1(C) Radio Receives Milestone Certification from JTRS Joint Program Executive Office”, 5 September, 2007.

[15] SCIP-232, Secure Communication Interoperability Protocol ECMQV/AES – NATO Cryptography Specification, V1.0.

[16] Jack Alvermann and Dr. Michael Kurdziel, SCIP IICWG White Paper: “SCIP Secure Voice Over 25 KHz LOS Tactical Radio Channels”, Revision 0.1, May 31, 2009.