Secure Communications Interoperability Protocols (SCIP)

John S. Collura
NATO C3 Agency
P.O. Box 174
2501 CD The Hague
THE NETHERLANDS

John.Collura@nc3a.nato.int

ABSTRACT

The concept of NATO Network Enabled Capabilities, (NNEC) including network-ready communications systems requires a fundamental shift in the paradigms and policies used by NATO and the NATO nations. Enabling these concepts down to the tactical mobile user community will be a challenge. Gone are the days where a single nation brings a combat-ready brigade to a NATO sponsored engagement. Modern brigade-level NATO deployed forces may consist of contributions from many nations. This can be highlighted by the fact that one nation might provide command and control capabilities, another logistics, a third special operations, etc. If communications equipments are purchased from multiple sources in multiple nations, and used in-theatre by the nations contributing to a multinational NATO Response Force formation, (brigade, battalion or corps) there are some inherent issues that require resolution to enable efficient network-ready interoperable communications systems. Adding to these issues are the requirements for secure communications and key management. Which nation or entity will provide the security authority in the deployed segment? Will it be the nation supplying command and control, security, logistics, or some other? Or will it be a NATO entity such as NATO HQ, JFHQ Lisbon, JFC Naples, JFC Brunsum, SHAPE, NAMSA, etc.? Who will be responsible for the in-theatre distribution of cryptographic keying material for the operation? When working with coalitions, how does one define communities of interest such that there is appropriate isolation of operations between different coalitions? Can capabilities be eliminated when a coalition member ceases to be friendly? Efficient net-ready interoperable communications systems are one of the core enabling capabilities for future effective NATO engagements.

The Secure Communications Interoperability Protocols (SCIP) represent the next generation NATO interoperability protocols for flexible high grade secure end-to-end (voice and data) communications. These communications protocols enable end-to-end application layer security, regardless of the underlying bearer networks and infrastructures. Indeed, the protocols rely on the commercial and/or military infrastructure and associated standardized inter-working functions that enable communications between differing networks (ISDN, PSTN, GSM, etc.). While currently fielded equipments in the US are primarily based upon circuit-switched transport infrastructures, ongoing research will eventually produce interoperable equipment based upon packet-switched transport infrastructures using IP-based security. These same protocols, if included in the various national software-defined radio programs, can provide the capability of securely integrating tactical networks into the existing interoperable strategic communications infrastructures.

NATO is currently investigating how the SCIP protocols can best provide secure interoperable communications for both tactical and strategic operations. Current technologies address strategic communications on both wired and wireless platforms. Future needs require that these same devices be interoperable with tactical military communications systems (characterized as mobile, low bandwidth, LPI/LPD) as well as IP-based or circuit switched communications systems.

Collura, J.S. (2006) Secure Communications Interoperability Protocols (SCIP). In *Military Communications* (pp. 19-1 – 19-10). Meeting Proceedings RTO-MP-IST-054, Paper 19. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Secure Communications Interoperability Protocols (SCIP)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **NATO C3 Agency P.O. Box 174 2501 CD The Hague THE NETHERLANDS**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202750. RTO-MP-IST-054, Military Communications (Les communications militaires), The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**10**	

The US has sponsored an International Interoperability Control Working Group or I-ICWG for all participating NATO member nations to come together and work on common solutions. These solutions address both signaling and cryptographic issues (including key management), and are based upon validated NATO requirements as generated by the nations through the NC3B substructures, SHAPE and ACT. Through this I-ICWG, any NATO nation can bring national as well as common requirements to be considered in a single forum. SCIP has one overarching signaling plan for NATO and national signaling requirements. This should result in dramatically reducing the burden of configuration management. Both signaling and cryptographic requirements are addressed by the appropriate NATO bodies, and fed to the I-ICWG for the generation of common interoperable NATO high grade solutions. The common NATO approach adopted by the SCIP protocols can enable private solutions to national sovereign requirements resulting in reduced life cycle costs for the key management infrastructure required to support national modes.

This paper will address some of the challenges involved with the SCIP program, and will provide insight into how these challenges can contribute to the future network-enabled world of Alliance deployments. Future integration of end-to-end application layer security with domain-to-domain network layer security will be discussed, if not resolved.

1.0 BACKGROUND

Over the past 20 years, NATO has achieved interoperable secure voice communications through the use of the Narrow Band Secure Voice II (NBSV-II) series of equipments. There were four equipments produced to a common standard by independent manufacturers in different nations. These NBSV-II equipments operate over the homogeneous analog PSTN network using either common key material for NATO communications, or private key material for national communications. The NBSV-II devices are only capable of using pre-placed key material, with common key sets for all NATO entities requiring secure communications. Using separate key sets, the NBSV-II devices enable secure communications for national sovereign purposes. This type of operational scenario does not support modern day network-enabled operations where dynamically negotiated session keys provide confidentiality, authentication and data integrity.

Recently NATO has grown in size to 26 nations, and has been assigned responsibility for many different operational engagements (KFOR, SFOR, ISAF, etc…). This growth in both membership and mission is accompanied by additional demands on allied communications systems for reach-back from the deployed segment to both NATO (HQ, SHAPE, ACT, JFC Brunsum and JFC Naples) and national capitals. Allied communications in NATO's deployed segment are characterized by coalition operations requiring distinct Communities of Interest (COIs) that are dynamic in nature. Coalition allies may at some point no longer have the "need to know", necessitating their removal from coalition operations information sharing.

2.0 SCIP

The Secure Communications Interoperability Protocols, SCIP, are a collection of application layer interoperability protocols designed to enable end-to-end secure voice *and/or* data communications across heterogeneous commercial and military bearer infrastructures and networks. Regardless of whether this communication is voice or data, an end-to-end data link is required. The minimum requirement calls for a 2400bps synchronous data channel from point A to point B to be established to provide a secure communications channel. Secure voice communications use this data channel to transmit an encrypted digital representation of the speech signal across a concatenation of bearer networks. With higher channel capacity, the SCIP protocols allow for higher data rate voice coding algorithms, or higher rate data transmissions. The SCIP approach to secure interoperability is application layer oriented, and as such is independent of the underlying network. The independence of specific communications bearer

technologies embraces both the evolutionary and (potentially) revolutionary developments of communications systems, networks and technologies. The SCIP protocols support a broad, network-independent architecture that implements specific technologies (currently PSTN, ISDN, CDMA and GSM). Individual SCIP products implement distinct subsets of this architecture based upon whichever commercial or military communications system provides the bearer network for that specific architectural segment. The SCIP protocols depend upon standard commercial (or military to commercial) Inter-Working Functions (IWFs) to translate the signals across the heterogeneous bearer networks. Network independence enables the SCIP protocols to embrace new technologies and protocols as these technologies and protocols mature and new ones appear. The SCIP standard relies on a uniform signalling plan for NATO and the NATO nations to build equipments compliant to the SCIP standard. By following a unified signalling plan integrated with both NATO and National cryptographic specifications, this enables the nations to use the SCIP standard for both NATO and national sovereign requirements. National sovereign communications requirements need not be shared with the NATO community. These national signalling specifications would then become a private national signalling annex to the common NATO signalling plan.

A typical SCIP scenario might have an end-to-end communication originate on a CDMA based cellular telephone (North American standard) and terminate on either a GSM cellular telephone or an ISDN telephone. In either case, the SCIP data signal traverses the CDMA mobile infrastructure from the handset to a base station and is translated from the IS-95 CDMA protocol stack to a V.32 modem signal for transmission over either a PSTN or an ISDN channel. Finally, the signal is then converted from the V.32 modem signal to the GSM signal (at the closest base station to the receiving GSM mobile handset) and transmits out to the mobile unit where the signal is decoded into either digital voice or data. In the case of the ISDN network, the V.32 modem signal would be converted back to the voice or data stream at the end terminal.

Both national as well as NATO secure voice requirements can be satisfied using SCIP-enabled products. The interoperability model created by the NBSV-II equipments is extended by the SCIP concept. The NBSV-II program was founded upon a homogeneous commercial infrastructure (PSTN) and established Communities of Interest (COIs) using interoperable equipment coupled with distinct key sets, NATO key for NATO communications and national key for national sovereign purposes. SCIP expands this concept by enabling secure end-to-end communications across a variety of bearers. Furthermore, any number of COIs can be established using multiple traffic encryption algorithms, both common and private protocols, and key materials. The critical point is that every nation must implement the identical call setup procedures, and at least one interoperable cryptographic mode. To provide maximum flexibility, the nations should implement two interoperable NATO cryptographic modes, the NATO secret (non-published) traffic encryption algorithm for NATO communications, and the AES public (widely published and available) traffic encryption algorithm for coalition operations.

3.0 CRYPTOGRAPHIC DEFINITIONS

3.1 Symmetric Key Material

NATO has historically achieved secure communications in the deployed segment using symmetric key material, also known as pre-placed key. It is called symmetric because every unit in the communications network has identical copies of the key material. Symmetric keys suffer from two main weaknesses, both associated with key management. First, if any key in the communications network is compromised, all communications on that network are compromised, including past transmissions using the same net key which may have been recorded. The compromise endures until either the end of the crypto key period, or the compromise is discovered and all units are re-keyed. The second weakness lies in the manual distribution of the key material itself. As stated above, if the key is compromised, all units must be

re-keyed. Since NATO distributes symmetric key manually, this is a costly and labor intensive task. The strength in a symmetric key configuration lies in the ability to configure large multiparty conferences without elaborate key exchange procedures. It must be noted however, that this is a minor portion of current communications with separate cryptographic key sets.

3.2 Asymmetric Key Material

Asymmetric Key negotiation provides each side of a secure communication with unique key material valid only for that session. In this type of key provisioning system, each side has a public and a private cryptographic key component. A "trusted authority" (also known as a Certification Authority or CA) must also issue authentication certificates (signed version of the public key component plus other info) to all secure communications equipments and/or users. The first step is for the two sides of the communication to exchange authentication certificates to prove to the other side that they are both valid users. After authentication, each side performs an algebraic operation to their public component, and transmits that information in the clear to the other side. Upon receipt, this public information is combined with that sides' private component to derive a unique symmetric session key. With this type of key derivation scheme, each side of the communication has a distinct key from the other side. The strength of this system lies in the unique session keys as opposed to the common shared key as in a symmetric pre-placed key system. The Electronic Key Management System (EKMS) required to update the master keys (both public and private) makes the asymmetric key negotiation much more flexible than the Symmetric system, with dramatically lower life cycle costs. There is currently no known method of extending this type of key negotiation beyond two parties, therefore, the only option for secure multiparty conferencing is to use pre-placed key.

3.3 Electronic Key Management Systems, EKMS

"EKMS is a generic name for the electronic distribution of cryptographic key and key management services. In the US, EKMS is a key management, COMSEC material distribution, and logistics support system consisting of interoperable Service and Civil Agency key management systems. The US EKMS program was established to meet multiple objectives, which include supplying electronic key to COMSEC devices in a secure and timely manner and providing COMSEC managers with an automated system capable of ordering, generation, production, distribution, storage, security, accounting, and access control. Other features of the US EKMS system include automated auditing capabilities to monitor and record security-relevant events, account registration, and extensive system and operator privilege management techniques that provide flexible access control to sensitive key, data, and functions within the system. The common EKMS components and standards will facilitate interoperability and commonality among the Services."[1] The NATO Military Committee Distribution and Accounting Agency or DACAN has the responsible for providing NATO and the NATO nations with this same capability. The NATO EKMS system is known as DEKMS, or DACAN provided EKMS.

3.4 Certificates and Trusted Authorities

A certificate is a digital document that attests to the binding of a public key (to either the identity of the user, or a particular device) on both sides of an electronic key negotiation or exchange. In addition, it verifies the authenticity of the public key and provides non-repudiation to the exchange. A Certification Authority (CA) is a trusted authority that issues a certificate used to authenticate the identity of users under its authority with a given public key. In addition, each time a unit performs a re-key of the master keys, the CA provides that unit with an updated Certificate Revocation Lists (CRL)[1]. A Certificate Revocation List is simply a list of certificates where the private component of the Certificate based key

[1] Older non certificate based key management systems used Compromised Key Lists (CKL) rather than CRLs, but the functionality was the same.

has been disclosed, was feared disclosed or lost, became inoperative, or for any other reason should no longer be taken as valid. The CRL is an integral part of the EKMS system required to remove the trusted association from compromised equipments or keys, rendering them incapable of participating in a secure communication.

3.5 Encryption Suite A and Suite B

Following the guidelines set forth by both crypto modernization and common criteria, NATO is currently working on the definition of requirements and solutions for two NATO centric cryptographic suites referred to as "A" and "B". Suite "A" is for NATO to NATO communications using a secret non-published traffic encryption algorithm and all of the associated components required to make that mode operational. Suite "B" is primarily for NATO to Coalition communications, but may include NATO to NATO communications up to a certain classification level. Suite "B" will use the Advanced Encryption Standard as the public traffic encryption algorithm and all other components required to make that mode operational. Note that both symmetric and asymmetric key types can be used with either Suite "A" or "B", and that the approach advocated for the SCIP protocols should be the same for other programs and protocols such as IPsec.

3.6 Communities of Interest (COIs)

Cryptographic Communities of Interest are defined by certificates sharing a common trust relationship or key set. In an asymmetric scenario, a part of this relationship is the ability for the public and private keys within that group to negotiate unique session keys. It is possible to isolate cryptographic communities through the manipulation of these trust relationships and in the design of the public and private key components. It is important to note that COIs are created and used to isolate the members of each group from access to communications with the members of the other groups. In other words, the NATO community of interest enables NATO member nations to communicate with each other, or with a coalition. In contrast to this, a national sovereign COI would isolate the communications of that nation from communications with the rest of NATO. These various COIs can be created using various means, including the traffic encryption algorithm, the universals used to define the public and private components of an asymmetric exchange, a pre-placed group key, etc.

4.0 DEPLOYED OPERATIONS

NATO deployed operational responsibilities and capabilities are evolving at a rapid pace to allow the Alliance greater flexibility and options when dealing with a range of problems requiring NATO responses. These responsibilities include Conflict Prevention, Peacemaking, Peacekeeping, Peace Enforcement, Peace Building, Civilian-Military Cooperation (CIMIC) and Humanitarian Operations. The tools available to NATO range from diplomacy, non-combat operations up to full military engagements in support of an article 5 conflict.

Effective Command and Control lie at the heart of any successful military operation. The NATO nations have chosen the Combined Joint Task Force Head Quarters (CJTF-HQ) concept for Command and Control in the deployed segment. "A CJTF is defined as a Combined (multi-national) and Joint (multi-service) deployable task force tailored to the mission and formed for the full range of Alliance military missions.

The NATO Response Force (NRF) provides the Alliance with a range of options to deal with the diverse set of NATO missions through the establishment of three main force structures. These include the Very High Readiness Forces or VHRF, the High Readiness Forces or HRF, and the Low Readiness Forces or LRF. The VHRF is up to Battalion in size, is deployable within 5 days and is intended to provide a rapid

initial NATO response. The HRF is up to Brigade in size and is deployable within 30 days and is intended to provide sustained NATO operation. Finally, the LRF is up to corps in size, deployable within 60 days, and is intended to allow NATO to maintain the deployed operations. Each of these NRF formations has either a Combined Joint Task Force (CJTF) HQ or a Deployed Joint Task Force (DJTF) HQ.

NATO forces have recently been engaged in multiple operations ranging from peacekeeping as in the KFOR, and SFOR missions, to peace enforcement as in the Afghanistan (ISAF) mission. Future NATO-led missions involving the NRF will require increasingly higher states of readiness, integration, interoperability and mobility. The multi-national battalions, brigades and corps that make up the NRF formations have challenges that are not generally encountered when the forces of a single nation are assigned a mission. Some of these challenges may be overcome by more intensive training, while others may require shifts in national policy and infrastructure to enable effective solutions to be developed and fielded.

4.1 Secure Interoperability

This section provides a contrast between currently deployed NATO communications systems, and projected future NATO communications capabilities and concepts. These differences should highlight NATO's inability to work effectively in a Network Enabled Capability (NEC) world using current approaches. The current coalition operations in Iraq and Afghanistan are good examples of the difficulties in establishing effective communities of interest using current communications infrastructures and techniques. The US currently maintains over 84 independent communications networks in support of coalition operations. These solutions are redundant and require the information to be sharable to the lowest common denominator.

4.1.1 Current Approaches

Secure communications to the deployed operational environment remains one of the most challenging services to provide in a multinational environment. Nations invest in tactical communications equipment built to a common set of NATO STANdards AGreements (STANAGs) such as voice coders like the STANAG-4591 Mixed Excitation Linear Prediction (MELPe) algorithm and on-air waveforms, (GSM, ISDN, HF, VHF, UHF) etc. While most nations build equipments that interoperate in the clear using these STANAGs, they rarely interoperate ***securely*** and efficiently when used in a multinational environment. Since each nation equips its forces based upon national sovereign requirements, each nation implements national cryptographic solutions rather than common NATO solutions. The result is secure equipments that do not provide secure interoperability across multinational boundaries. To offset this condition, the current solution is for the forces of one nation to "hand receipt" communications equipment and cryptographic key material to any forces (NATO or otherwise) they are required to communicate. This often leads to situations where NATO forces are using unfamiliar secure communications equipments.

A good example of this is the current rotational command structures in ISAF where a lead nation assumes command of a multinational brigade for a period of 6 months. With each rotation, the lead nation supplies all Communications and Information Systems (CIS) equipment required to support the mission. This means that the lead nation must supply an entire multinational brigade with secure communications infrastructure (radios, networks, cryptographic key, etc.). Each new command nation has a different infrastructure from that of the previous lead nation. With this new infrastructure comes the inevitable period of integration with the NATO command infrastructures, both above and below the deployed CJTF command HQ. There is also a period of acclimation to using unfamiliar gear and procedures (especially for the subordinate multinational units). This is complicated by the connectivity points defined in NATO STANAG 5048 which defines up to what point NATO provisions the communications infrastructure. Below that point, the lead nation must supply the equipment.

There are policy issues that must be resolved related to the interconnection of NATO and national networks. NATO policy currently requires three independent networks providing CIS IP connectivity, one for NATO Secret, one for Mission Secret, and an unclassified network. The Mission secret network is a private network dedicated to in-theatre operations. To achieve reach back to NATO commanders and planners, the mission secret network must be connected to the NATO secret network via some form of gateway technology.

NATO is operating in theatres where CIMIC (CIvilian-MIlitary Co-operation) or emergency humanitarian assistance operations are required. NATO CIMIC is defined as the co-ordination and co-operation, ***in support of the mission***, between the NATO commander and civil actors. This includes national populations and local authorities, as well as international, national and non-governmental organizations (NGOs) and agencies. NATO CIMIC and humanitarian missions are independent as the humanitarian assistance mission is usually carried out in coordination with various NGOs (such as the International Commission of the Red Cross (ICRC), The Red Crescent Organization, Médecins Sans Frontières (MSF), the World Food Program (WFP), etc.) and is not directly supporting the mission. Whether NATO is working a CIMIC mission, or in coordination with an NGO, field commanders must have reliable communications with appropriate civil authorities. To enable these communications today, NATO forces carry Professional Mobile Radios (PMRs) (TETRA, TETRAPOL or APCO-25) in addition to the secure military radios required for secure NATO communications. To maintain their strict neutrality, most NGOs do not currently allow encrypted communications. One potential solution to this problem is for both PMRs and military radios to include common interoperable SCIP modes.

4.1.2 Future Approaches

The NATO nations are exploring the SCIP protocols as a viable solution for interoperable end-to-end secure communications across NATO and national infrastructures. The current set of SCIP signaling protocols enable secure interoperable communications across PSTN, ISDN, GSM and CDMA networks. These protocols are evolving to include secure interoperability to military radio protocols, Professional Mobile Radio protocols, as well as cross domain solutions with secure wired and wireless LAN IP technologies. It is crucial for NATO to resolve how to provide authentication for certificates originating on an application layer (as in SCIP) and terminating on a network layer (as in IPsec). The current approach is to “tunnel” a SCIP signal through an IPsec infrastructure. Two current US programs will enable secure communications across the application to network layer divide. These are the Secure Terminal Equipment (STE) and the SECNET-54 Secure Wireless LAN equipment. Through the INSC (Interoperable Networks for Secure Communications) program, Germany is investigating how to provide Authentication services across the application to network layer. These and future equipments and programs from the other NATO nations will provide the basis for secure cross domain interoperability.

When the NATO nations begin to field SCIP-enabled equipment, the difficulties and life cycle costs associated with multinational interoperable secure communications will drop substantially. Additional reductions in life cycle costs may be derived if nations adopt common signaling and key management approaches for national sovereign modes. A crucial part of future NATO capabilities lies in the use of electronic asymmetric key, and in its delivery and maintenance using an EKMS system. EKMS infrastructure can provide a limited capability to locally generate key material, act as a local Certificate Authority (under the root certificate authority), establish, update, and maintain the Certificate Revocation Lists (CRL), etc. Secure interoperability will be ensured by common call setup procedures, signaling and at least one common NATO cryptographic mode (Suite A) and one common coalition cryptographic mode (Suite B).

NRF operations based upon a combination of symmetric and asymmetric key will be much more flexible, responsive and effective. This flexibility is partly based upon the ability to remotely key devices, negotiate unique session keys, eliminate compromised radios or equipments from networked operations,

seamlessly integrate communications equipment from many nations, etc. Additional functionality is provided by ability to reconfigure equipments via software, and in the creation of NATO and coalition operation COIs. NATO and national operations by necessity require that information sharing follow the "Need to Share" doctrine. There may be a need to share certain information with the members of one coalition, and not another. For instance, NATO forces may need to share some form of operational data with coalition forces, but not with the NGOs working in-theatre.

Developments in the field of software defined radios (SDR) for military applications (US Joint Tactical Radio System (JTRS) or the UK Bowman Radio, etc.) provide the nations an unprecedented opportunity to bridge the secure interoperable communications gap. One of the strengths of the SDRs lies in the ability to reconfigure the radios to accommodate changing mission requirements. This is an oversimplification as each transmission band requires different antenna properties and configurations, and the various waveform algorithms require more or less computational power to transmit on these various bands. Each radio will be loaded with the features required to support a mission just prior to that mission. A key point to be noted is that the minimum configuration for the SDR is the capability of simultaneous transmission and reception on two separate bands. One band is used to support local mission communications, and another to relay the communications of other missions across the network. This feature is particularly useful for networked operations using dynamic key management in a NNEC NRF operational environment.

Consider a dynamic key management scenario where Software Defined Radios (SDRs) are used in a combat net radio operation or ad-hoc reconnaissance mission, and the pre-placed keys aren't available to all participants prior to the missions. Each SDR has a minimum of two channels, "a" and "b", where channel "a" is used for local net operations, (both voice and data) and channel "b" is used to relay communications traffic for other units. A secure communication can be established by temporarily "borrowing" bandwidth from channel "b" for a certificate based asymmetric key negotiation with a lead radio (or any radio in the network). Once this temporary secure link is established, the symmetric net key is transmitted to the new users. These new users can then join the secure communication as late entries using the SCIP protocols. Security is maximized in these scenarios because the strengths of both symmetric and asymmetric key material and authentication are employed. When the mission is over, then the session key expires and is destroyed, resulting in a less vulnerable overall system. This same technique can be used to establish and maintain a secure multi-media conference across a higher bandwidth geographically diverse network (both strategic and tactical). This is exactly what is required to enable network-centric operations to get the right information to the right person at the right time.

5.0 CONCLUSIONS

NATO Network Enabled Capabilities (NNEC) is fundamentally shifting how NATO and the NATO nations design, acquire and use secure communications equipment. The goal is to create a secure interoperable strategic and tactical infrastructure, regardless of which nation or company produces the CIS infrastructure. Trans-national cross domain security and interoperability must be enabled for effective and secure network enabled operations. The ability for the forces of any NATO nation to seamlessly integrate into the secure communications of a deployed NRF is critical to the success of any future operation. This capability will provide the authentication required to enable the NRF to achieve and prosecute the NATO Network Enabled Capabilities vision.

Policy issues such as security accreditation must be resolved to enable the NATO nations to operate in the security environment of the future. A case in point is the inclusion of multiple cryptographic algorithms in secure communications equipments slated for both national and NATO missions. A nation may decide to implement both NATO modes (suite A and B) as well as a national sovereign mode. At issue here is how to properly accredit the SCIP equipments for NATO and national use. The Military Committee SECurity and Accreditation AgeNcy (SECAN) is the only authority that can perform a security evaluation and

accreditation for NATO communications equipments. Likewise, it is up to the nation to perform its own security accreditation for the national modes. One important issue that must be resolved is how both a nation and NATO (SECAN) can evaluate equipments without compromising the integrity of the other evaluation. The nations must also work to bring their national policies in line with the future EKMS capabilities and allow NATO commanders, or those of another nation to provide key material for the common NATO modes, while at the same time provisioning national cryptographic key material through private national channels.

The SCIP protocols have been shown to provide many of the capabilities required to enable the concept of NATO Networked Enabled Capabilities. Future work within the NATO and international communities will enhance these protocols to provide greater integration of secure equipments while establishing separation through cryptographic communities of interest. Both national and NATO secure communications requirements will be served by the common approach known as SCIP.

6.0 REFERENCES

[1] Web citation: SPAWAR web site www.jya.com/don-ekms.htm