Open Framework for the NATO Secure Voice Strategy

Klaus-Dieter Tuchs, Ricardo Berto-Monleon,
Hermann Wietgrefe
NATO Consultation, Command and Control Agency (NC3A)
PO Box 174, 2501CD, The Hague, Netherlands
{klaus-dieter.tuchs; ricardo.berto-monleon;
hermann.wietgrefe}@nc3a.nato.int

Ammar Alkassar,
Timm Korte
Sirrix AG security technologies
Im Stadtwald D3.2, 22123 Saarbrücken, Germany
{a.alkassar; t.korte}@sirrix.com

Abstract— **The NATO Secure voice strategy identifies the Secure Communication Interoperability Protocol (SCIP) as the upcoming standard for secure voice communication within the NATO community. In support of the Secure Voice Strategy NC3A has been mandated to establish a NATO SCIP Validation Facility (NSVF) to enable conformance, interoperability and key management testing for NATO Nations. SCIP will enable multi vendor solutions for secure voice terminals, operating over heterogeneous networks, by using open standards.**

To tackle interoperability issues in secure voice communications for expeditionary operations, NC3A has developed a Secure Voice Platform using an open source voice switch. For enabling SCIP gateway functionality between circuit and packet switched networks a V.150.1 protocol stack as been added to the Secure Voice Platform. Due to its open design and flexibility the Secure Voice Platform is a very valuable resource in the conformance and interoperability tests for the integration of SCIP devices in NATO and national networks.

This article summarizes the NATO Secure Voice Strategy and the concept of the NATO SCIP Validation Facility. Focus is on the integration of the V.150.1 protocol stack in the Secure Voice Platform. Issues arisen during the integration process are addressed as well as those discovered and solved to address interoperability aspects.

SCIP, NATO Secure Voice Strategy, NATO SCIP Validation Facility,NC3A, Secure Voice Platform, Modem over IP, MoIP, V.150.1

I. Introduction

In a network centric environment voice communications are still an essential service for military planning and operation execution. Secure voice communication provides a service which is still unrivalled for its responsiveness, interaction and trustworthiness. In addition to the military role, in NATO secure voice is one of the key services used for political consultation. Therefore even in the current era of NATO network-enabled capability (NNEC) operations, secure voice remains an essential requirement.

Historically, secure voice implementations have been network technology specific, and vendor proprietary, combining communications and encryption process in a proprietary manner. NATO is therefore facing interoperability issues for secure voice services across the various national voice encryption solutions and heterogeneous voice network solutions. To mitigate the interoperability issues for NATO Response Force operations with rotating National contributions and their heterogeneous national voice encryption solutions, the concept of the Secure Voice Platform has been developed. The concept, however, still requires bespoke national encryption devices to terminate each encryption domain.

SCIP evolved from the Future Narrowband Digital Terminal (FNBDT) concept [1], is a promising concept that shall overcome the network service and vendor dependency of secure voice services. SCIP specifies the communication process for transmission, networking and key management, and separates the communication process from the encryption process via a standardized interface. This approach removes the interoperability issue from the network layer, while keeping all options to implement national or NATO encryption algorithms in SCIP compliant devices.

With SCIP equipment not being available yet, and Voice over IP (VoIP) becoming the de-facto standard for voice services in NATO, interim solutions for secure voice are implementing secured voice services as voice over secure IP connection. While this protects the content of a voice call against eavesdropping in the WAN, some pivotal features of a secure voice service can't be provided. Acknowledging the advantages of SCIP, the NATO Secure Voice Strategy outlines the path from current Voice over Secure IP provision towards SCIP provided end-to-end Secure Voice services.

In the following, the paper introduces the NATO Secure Voice Strategy, the role of SCIP in that strategy, and the resulting future secure voice architecture. Then, the NATO SCIP Validation Facility is introduced, and the Secure Voice Platform is presented. Finally, remain interoperability issues are discussed, and emerging work on this subject is presented.

II. NATO Secure Voice Strategy

A. Introduction

The NATO secure voice strategy addresses NATO's transition strategy towards network-enabled end-to-end (person-to-person or person-to-process) secure voice [2]. The strategy leads from the current position and addresses incremental transitions towards the desired end state of omnipresent secure voice.

978-1-4244-8179-8/10/$26.00 ©2010 IEEE

The NATO secure voice strategy has been developed in response to key drivers, namely:

- Evolving, diverse communication network technologies,
- Equipment obsolescence,
- Availability of new cryptographic technologies,
- Demand for wider interoperability,
- Need for simplified key distribution,
- Perceived inadequacies of many current secure voice solutions.

Today's communications networks and their associated technologies are changing at an ever increasing rate. Traditional real-time voice communication circuits are steadily being replaced by other technologies such as Voice over Internet Protocol (VoIP). On the other hand a dramatic increase in the use of mobile (e.g. cellular, GSM) phones has changed the way we communicate and users' expectations.

The requirement for secure voice communications adds an additional layer of complexity to this already challenging environment due to the additional stringent timing and reliability requirements for the synchronization of security protocols, cryptographic algorithm exchanges needed to support a real-time encrypted service and the need for a supporting cryptographic key management infrastructure.

B. *Secure Communication Interoperability Protocol (SCIP)*

SCIP has been identified by the NATO secure voice strategy as the future standard for secure voice communications at NATO. SCIP is developed to provide end to end encrypted voice and data communication between terminals operating on heterogeneous networks.

The SCIP specification is the result of the efforts of a multinational group involving NATO, national governments and industry. The SCIP specifications are available to nations and industry in order to develop interoperable secure voice and data terminals. As a result a SCIP terminal from vendor *A* in nation *X* will be interoperable with a SCIP terminal from vendor *B* in nation *Y* for end-to-end communications and security related communications. Only the encryption engine itself, and the related key material is selected and implemented subject to National or NATO requirements.

SCIP supports different voice codecs, the two key codecs are mixed excitation linear prediction-enhanced (MELPe) and G.729D. The MELPe voice coder offers state of the art voice coding, giving comparatively high voice quality and intelligibility from a 2.4 kbps channel. The G.720D codec offers better quality than MELPe but at the expense of using more bandwidth. G.729D operates at 6.4 Kbps.

SCIP terminals place some demands on the intervening networks, although in general these are only that the networks conform to the characteristics and interfaces defined in their respective standards e.g. Public Switched Telephone Network (PSTN) (V.32), ISDN (V.110), GSM (bearer service 26, BS26) etc. In providing SCIP over IP networks SCIP relies on standard VoIP services. Session initiation protocol (SIP) and real-time protocol (RTP) are both used by SCIP terminals to establish an IP connection between SCIP terminals [3]. SCIP over IP may be referred to as secure voice over IP (SVoIP).

SCIP was developed to operate over heterogeneous networks therefore the network interfaces must also support SCIP. This is of particular concern at the boundary between circuit-switched and packet-transfer networks. Here, SCIP uses the ITU-T standard v.150.1 [4]. SCIP uses only a subset of the V.150.1 standard therefore a SCIP standard covering the Minimum Essential Requirements (MER) for V.150.1 Gateways has been developed [5].

V.150.1 is commonly referred to as modem over IP (MoIP). Although this is an agreed international standard, it is not widely available and steps must be taken to ensure that military and commercial networks will be able to support SCIP across these interfaces.

C. *Future NATO Secure Voice Architecture*

Fig. 1 shows the envisaged future secure voice architecture where two scenarios will co-exist, one based on VoIP over an encrypted IP network, VoSIP (Voice over Secure IP) that will provide enclave-to-enclave encryption and another based on SCIP terminals operating on a variety of networks that will provide end-to-end (or terminal-to-terminal) encryption.

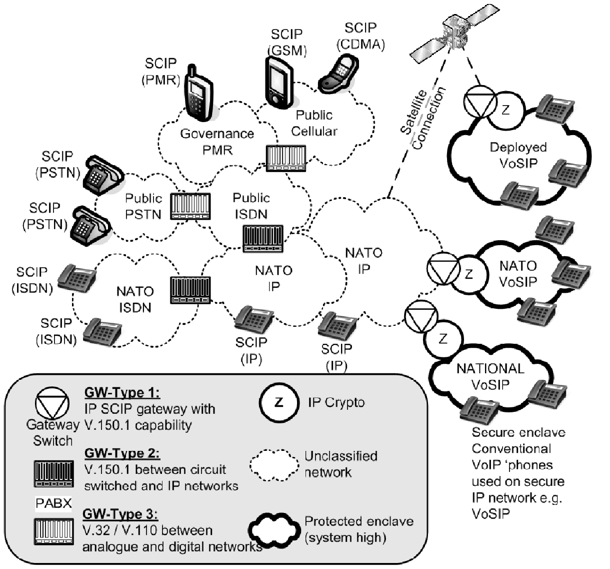

Figure 1. Upcomming NATO Secure voice architecutre

Three gateway types are identified by the NATO secure voice strategy for providing interoperability between the different networks:

- Gateway (GW) Type 1:
  GW supporting V.150.1 between VoIP and VoSIP which includes a SCIP encryption module to decrypt voice and forward the clear voice into the VoSIP network. This is a red gateway.
- GW Type 2:
  GW supporting V.150.1 to enable the transition of encrypted voice streams between ISDN and IP

networks. No voice encryption is performed in the GW.

- GW Type 3:
GW supporting V.110, V.32 and BS26 between ISDN and analogue PSTN as well as mobile networks like GSM and professional mobile radio (PMR).

The NATO SCIP validation facility described in the next Section III will emulate the complete variety of networks. The secure voice platform described in Section IV is designed to provide all three types of gateways described above.

III. NATO SCIP Validation Facility (NSVF)

A. Background

The success of a communication technology such as SCIP hinges ultimately on whether users can employ it to communicate as they wish, when they need, with whomever they chose.

The existence of the SCIP standard alone is not sufficient. Equipment built to the SCIP standard must be known to meet the standard. In addition, the ability of SCIP to operate over heterogeneous networks means testing must be performed to validate that the equipment operates over a wide range of networks.

The NATO strategy for SCIP recognizes the need for effective testing. This testing should have sufficient depth and breadth to give users and procurers of SCIP-compliant devices confidence that they will operate securely, reliably, effectively, and be interoperable with other SCIP-compliant devices in NATO strategic and mission environments.

The NSVF is located at NATO C3 Agency (NC3A) in The Hague and, applying NC3A experiences from other NATO testing and validation activities [7], performs the following tests for NATO Restricted as well as NATO Secret SCIP enabled devices:

- Conformance
- Interoperability and Network
- Key management

In order to be “SCIP compliant” a device shall successfully pass all three of the tests above.

The Minimum Interoperability Profile (MIP) [8] defines the minimum set of characteristics that a SCIP device must implement to be declared SCIP-compliant. The above mentioned tests are limited to the technical specification detailed in the MIP.

B. Conformance testing

The test procedures for conformance test are detailed in [9]. The conformance testing validates SCIP standard conformity of the Equipment Under Test (EUT). Conformance testing requires a SCIP compliant reference.

The SCIP community with the agreement of the International Interoperability Control Working Group – Technical Board (IICWG-TB), has agreed to use the General Dynamics SCIP Endpoint Tool as the reference SCIP enabled device to perform the conformance testing

C. Interoperability and Network testing

The fact that two devices operating in different networks are declared in conformance with the SCIP standard does not guarantee that they will be able to talk to each other. The Network and Interoperability Test guarantees the interoperability of different devices across various networks.

The networks used for the interoperability and network tests are drawn from a use cases matrix. Interoperability and network tests will ensure the interconnectivity of SCIP terminals across different networks and boundaries. Initially, interoperability and network testing is limited to interoperability over ISDN, PSTN, GSM and IP networks. These networks will also be interconnected via an intermediate simulated, repeatable, SATCOM link (see Fig. 2).

Interoperability and network tests will include delays, noise and other channel impairments that result from the aggregate characteristics of the channels and interfaces used in an end to end secure communication. It is necessary to assure the operational users of SCIP compliant devices can operate over typical NATO network connections, e.g. a double hop SATCOM link with associated delays. The complete test procedures are detailed in [10].

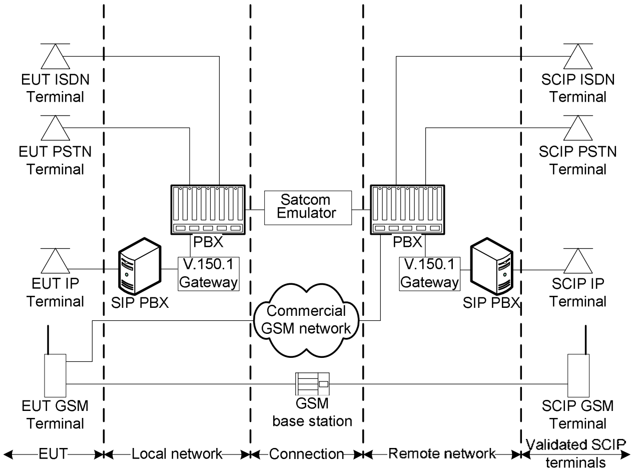

Figure 2. Interoperability and Network testing lay-out

D. Key Management testing

Key Management testing will be performed to verify that SCIP-compliant devices meet all of the requirements necessary to load and rekey key material supplied by the key management infrastructure. The general format of a test will be to fill a device with key, make a rekey call, and verify proper updating of the key material and Compromised Key List (CKL). A CKL is distributed along with the key material by the key management infrastructure, and consists of a list of compromised terminals that SCIP-compliant devices are no longer allowed to communicate securely with. During infrastructure testing both positive and negative tests will be used in order to test all aspects of key update and CKL processing.

E. NSVF Equipment

In order to perform all the above mentioned tests, the NSVF is furnished with the following equipment:

- Commercial V.150.1 SCIP Gateway,
- GSM Pico-cell,
- SATCOM simulator,
- General Dynamics SCIP Endpoint and Test Tool.

F. Available Network Interfaces

The NSVF must be able to support any network for which a SCIP device is developed. However it is impractical to configure a test laboratory with all necessary networks or network simulators at the outset. To solve this issue the NSVF provides trunking interfaces in accordance with the appropriate STANAG. It also provides terminal interfaces for the most common networks.

This solution allows any vendor to test its SCIP device regardless of its network interface as long as the vendor provides a network adapter to one of the offered interfaces.

The full list of interfaces available in the NSVF is provided below:

- ISDN:
  In accordance with STANAG 4578 Edition 3 for COMMERCIAL mode and using commercial interfaces; E1 in accordance with ITU-T G.703;
  RJ-45 in accordance with S0 interface.
- PSTN:
  RJ-11 2-wire, A-B interface.
- IP:
  In accordance with STANAG 5067, support for C1 interconnection point, Ethernet RJ-45 in accordance with 100 BASE-T interface.
- V.150.1.
  In accordance with SCIP 216 [5].
- GSM in the 900/1800/1900 MHz bands:
  9.6 kbps asynchronous transparent Circuit Switched Data (CSD) mode (GSM BS26).

IV. SECURE VOICE PLATFORM

A. Background

The Secure Voice Platform (SVP) is developed by NC3A as a flexible development kit which offers a mature set of building blocks to develop prototypic products in the area of secure voice communication. NATO's Deployable Communication and Information Systems Programme of work (DCIS, see also[12], [13]) developed the SVP concept, first addressing the requirement for secure voice interoperability for NATO Response Force (NRF) operations, where NATO secure voice services need to interoperate with various national secure voice systems. To break and interconnect the various bearer and encryption domains for a force rotating every six month, a flexible solution was needed, easily adaptable to changes in the multinational force composition. Responding to related secure communication requirements, a number of prototype solutions have been developed since then, and successfully tested during interoperability exercises: Secure Voice Gateway (SVG), Information Exchange Gateway Voice Module (IVM), Secure Conferencing Facility (SCF) and the Secure Protocol Gateway (SPG).

The flexibility of the SVP is based on the use of open standards and platforms. For the use of the SVP in a SCIP environment a V.150.1 protocol stack was required which is not available as an open source implementation. Therefore it was decided to extend the SVP with a V.150.1 in-house development which is described in Section V. The core components of the SVP are based on open platform architectures running on GNU General Public License.

The modular platform of the SVP allows building all gateway types identified by the NATO secure voice strategy, and most of the physical interfaces required for the NSVF are already available in the SVP. Therefore it was decided to propose the SVP as the main platform to provide the required gateway functionality for the NSVF.

The following sections introduce the functional blocks of the SVP.

B. Functions

The secure voice platform (SVP) builds a flexible architecture consisting of five main functions which can be combined and configured to fulfill various product requirements:

- Operating system function,
- Security framework function,
- Voice switching function,
- Network interface function,
- Gateway configuration management function.

Fig. 3 provides an overview of the functions and some essential sub functions of the SVP.

1) Operating System

The operating system is based on a secured Red Hat Enterprise Linux 5 Server® (RHEL5) fulfilling the Evaluation Assurance Level (EAL) 4+. The fulfillment of the Common Criteria with an Evaluation Assurance Level (EAL) 4+ provides the baseline for accreditation once the SVP will be turned into a product.

2) Security Framework

The operating system of the SVP controls access to all hard- and software components grants user access to the SVP. The security features of the EAL4+ RHEL 5.1 Server version are based on two main parts:

- Restricted configuration of Linux system;
- Policy based access and runtime control with SELinux.

Access control to the SVP is provided by the Linux system while the policy enforcement is performed by SELinux. SELinux is a security module developed by the National Security Agency (NSA) and published as Open Source software [6] and builds the basis for the security of the SVP. All running processes are controlled by SELinux.

SELinux denies all actions from the software which are not explicitly allowed by the SELinux policies. Adding additional software to a SELinux controlled system means that this software is not able to do anything if no valid SELinux policy exists. This means for an accreditation process that the evaluators need to evaluate the extra policies written for this software not the software itself which reduced the complexity of the evaluation process. For the integration of the Secure Voice Platform additional SELinux policies for the voice switching system (see Section 3), the gateway configuration management (see Section 5) and the Modem over IP Integration (see Section V) were developed.

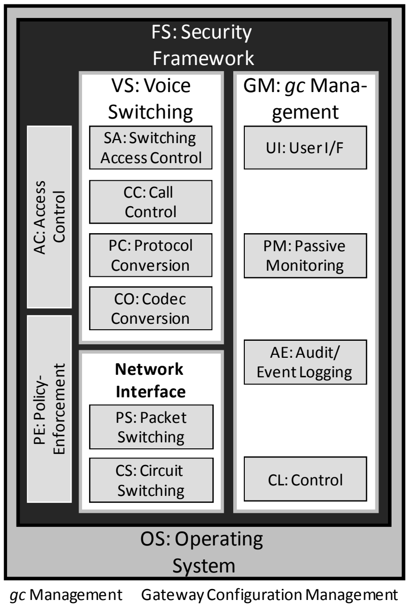

Figure 3. SVP main function blocks

3) *Voice Switching*

The core functionality of the SVP is the voice switching functionality. The voice switching function is provided by an Asterisk® 1.4 platform. Asterisk has a modular design which enables a straight forward adaption to changed requirements. A large number of modules are available for the Asterisk system because of the large user community.

If specific requirements cannot be fulfilled from available modules it is possible to develop and integrate new modules because of the open source nature of the product. For SCIP compatibility reasons the requirement of a V.150.1 protocol stack was identified. This protocol stack is not publicly available for the Asterisk™ system so it was decided to start the development. Details about the development are shown in Section V.

4) *Network Interface*

Network interfaces integrated in the SVP are dependent on the hardware used for product implementation. The Ethernet interfaces are usually integrated in the PC platform used for a specific implementation while the circuit switching interfaces like ISDN BRI/PRI and analogue interfaces provided by specialized products integrated on the PC platform. The interfaces used internally for interconnection the circuit switching cards are usually the internal Peripheral Component Interconnect (PCI) bus or USB (Universal Serial Bus) bus of the PC.

5) *Gateway Configuration Management*

The management functionality is a critical aspect for the use of the SVP in a deployed environment. To ease the configuration of the system, the users in the field need to be enabled to configure only those parameters which are essential for the mission. Therefore a specialized Gateway Configuration Management (*gc*M) tool was developed by NC3A reducing the complexity to the required minimum.

The *gc*M is realized by a client – server architecture. The Gateway Configuration Server (*gc*S) is running on the SVP itself and has access to all configuration and logging files on the SVP. The Gateway Configuration Client (*gc*C) can be installed on any PC and is capable of controlling and monitoring the SVP remotely. The *gc*C provides an intuitive Graphical User Interface (GUI) for the user and hides the complexity of the SVP configuration from the user.

V. V.150.1 / MODEM OVER IP INTEGRATION

The purpose of the V.150.1 integration is to extend the capabilities of the SVP in order to act as a MER compliant gateway, linking SCIP devices in different networks together.

The integration has been realized smoothly into the Asterisk™ switching core. While the central switching core is independent from the network technology, the interfaces implementing the actual protocols are handled by so called "channel drivers". While a number of channel drivers for voice communication over ISDN (Chan_Sirrix) and analogue line cards (Chan_dahdi) as well as for SIP (Chan_sip) and H.323 exists, there is no direct support for data communications for the communication subsystem available.

The V.150.1 integration, realized in these efforts, consists of two separate channel drivers that implement the two sides of a standard V.150.1 connection. On the one side, this is a module capable of handling analog modem (V.32/V.34) connections (Chan_V3X). Analogue modem calls can be terminated at the SVP with internal or external modems, it was tested with external USB modems.

The second module includes a complete SIP stack for VoIP signaling as well as the actual V.150.1 IP-side Simple Packet Relay Transport (SPRT) protocol implementation (Chan_MoIP). The concept of the V.150.1 integration is shown in Fig. 4.Each of these modules consists of a small channel driver in order to interface with the Asterisk core and a software library containing the technology specific functionality.

The V.150.1 standard itself offers a multitude of possible protocol extensions and features from which the most important ones were chosen and described in the SCIP-216 document [5]. Even with those requirements in place, there was still enough uncertainty for different vendors to come up with different - and incompatible - implementations.

The most notable issue in this area, is the lack of a binding specification for the actual IP transport of the V.150.1 protocol (SPRT) data. When using SIP as a signaling layer, it is possible either to transport the V.150.1 payload data over the same UDP port as the standard RTP media stream - or use a different UDP port for these packages. In order to be compatible to both implementations both versions where implemented, including an auto-detection mode to switch between the two possibilities on demand. Using the SVP V.150.1 implementation, successfully established SCIP encrypted calls between analogue and IP-based SCIP devices. For the first time, it was possible to link two SCIP devices with different incompatible IP transport implementations as mentioned above.

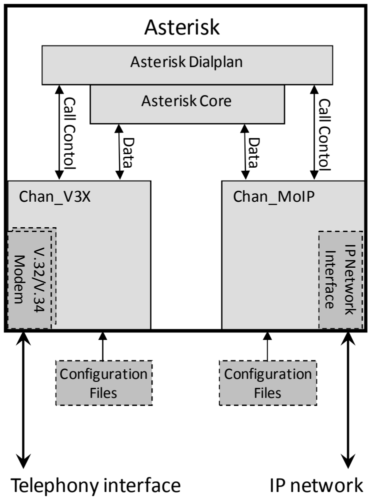

Figure 4. Concept diagramm of V.150.1 integration

The modular approach allows the system to be easily extended by other modules in order to for example provide V.110 to V.150.1 for ISDN or GSM/CSD to IP conversion in the future. A seamless integration of the V.150.1 implementation in the *gc*M tool is performed by integrating the V.150.1 configuration files into the *gc*M.

VI. SCIP Interoperability Issues

Already during the implementation phase of the V.150.1 protocol in the SVP a number of interoperability issues were detected:

- Timeouts caused by modem connections:
  A modem connections on analogue lines requires a reasonable long time (20-30s) to establish a connection. This can cause timeouts on involved SIP trunks, gateways and other components especially in an IP environment were such long delays are not typical.
- Standard options:
  The V.150.1 standard offers variants for connections setup. This needs to be reduced by the related SCIP standard [5] by defining only one valid possibility for establishing a call. This reduces interoperability issues during the call setup phase.

The detected interoperability issues are influencing the SCIP standard definition.

Using open platform implementations like the SVP in the SCIP environment allows fast adaption to identified interoperability issues. E.g. the mentioned timeout problems in the public network could be solved by configuring the SVP in such a way that connections are signaled back as successfully established even though the modem call was still in the establishment phase. Such workarounds on standard gateways would not be possible without the involvement of the manufacturer.

VII. Way ahead

The SVP as a flexible development platform for prototypes supporting secure voice is under constant enhancement. Planned development steps of the SVP are:

- Digital Signal Processor (DSP) integration for terminating modem connections directly on the SVP without use of external modem banks;
- V.110 support for direct interconnection e.g. to ISDN and GSM networks.

The NSVF is finishing its arrangements to be operative by the end of Q3 2010 to perform Conformance and Network and Interoperability tests for NATO Restricted and NATO Secret devices. Key Management tests it will be ready by the end of 2010 to perform tests on NATO Secret devices.

References

[1] Daniel, E.J. Teague, K.A. Sleezer, R. Brewer, J. Raymond, J. Beck, W.J. Hershberger, J.; "The Future Narrowband Digital Terminal", The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002, pp. II-589 - II-592 vol.2.

[2] M. Street, B. Bottesini, R. Russo, P. DeLaere, G. Elzinga, R. Murtland, "Providing Interoperable Secure Voice in Converging Heterogenous Networks", Military CIS Conference, Prague, Czeck Republic, September 2009.

[3] L. Velasco and M. Street, "Performance of SCIP devices on public and classified heterogeneous networks", Military CIS Conference, Krakow, Poland, September 2008.

[4] International Telecommunication Union – Telecommunication Standardization Sector Recommendation V.150.1, "Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs", ITU-T, Geneva, Switzerland, 2004.

[5] SCIP-216 Rev 2.0 "Minimum Essential Requirements (MER) for V.150.1 Gateways", SCIP International Interoperability Control Working Group, November 2007.

[6] National Security Agency (on-line), http://www.nsa.gov, Security-Enhanced Linux, at http://www.nsa.gov/research/selinux/, Januar 2009.

[7] Alberto Domingo, "A Reference Testbed for the Experimentation, Testing and Validation of NATO Communications and Information Systems" in IEEE TridentCom 2007, Orlando, FL, May 2007

[8] Minimum Interoperability Profile, SCIP-221 document

[9] NATO Consultation, Command and Control Agency Test Documentation SCIP-610 V.1.0, "ConformanceTest Plan", The Hague, Netherlands, October 2010 (NATO Unclassified).

[10] NATO Consultation, Command and Control Agency Test Documentation SCIP-620 V.1.1, "Interoperability and Network Test Plan", The Hague, Netherlands, February 2010 (NATO Unclassified).

[11] Ammar Alkassar and Christian Stüble: "A Security Framework for Integrated Networks", in IEEE, MILCOM 2003, IEEE Military Communications Conference in Boston, October 2003.

[12] L. Bastos, H. Wietgrefe, "WiMAX for Highly Deployable Mission-Critical Communications Networks", MILCOM 2007 Conference, Orlando, 29-31 October 2007.

[13] Luis Bastos, Hermann Wietgrefe: "WiMAX at Traffic-Demanding Electronic Warfare Air Exercise ELITE 2008", in IEEE Military Communications Conference in Boston, October 2009.