

NATO UNCLASSIFIED

NATO STANDARD

AComP-5068

SECURE COMMUNICATIONS INTEROPERABILITY PROTOCOL (SCIP)

**Edition A Version 3
NOVEMBER 2020**



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED COMMUNICATION PUBLICATION

**Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN**

NATO UNCLASSIFIED

NATO UNCLASSIFIED

INTENTIONALLY BLANK

NATO UNCLASSIFIED

NATO UNCLASSIFIED


NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

18 November 2020

1. The enclosed Allied Communication Publication AComP-5068, Edition A, Version 3, SECURE COMMUNICATIONS INTEROPERABILITY PROTOCOL (SCIP), which has been approved by the nations in the Consultation, Command, and Control Board (C3B), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 5068.
2. AComP-5068, Edition A, Version 3, provides one additional reference module, SCIP-214.7, and an update of reference module SCIP-214.6. SCIP-214.7 is a way to transmit SCIP information encapsulated within V.14 and formatted as ITU V-series modem signaling and the resulting modem samples finally encapsulated within a G.711 codec transmitted over an RTP (or SRTP) IP packet. SCIP-214.6 is dedicated to the interoperability with the Tactical Secure Voice Cryptographic Interoperability Specification (TSVCIS).
3. AComP-5068, Edition A, Version 3, is effective upon receipt and supersedes AComP-5068 , Edition A, Version 2, which shall be destroyed in accordance with the local procedure for the destruction of documents
4. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (<https://nso.nato.int/nso/>) or through your national standardization authorities.
5. This publication shall be handled in accordance with C-M(2002)60.

for 
Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

NATO UNCLASSIFIED

NATO UNCLASSIFIED

INTENTIONALLY BLANK

NATO UNCLASSIFIED

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

[illegible]

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

[illegible]

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1-1
1.1. BACKGROUND	1-1
1.1.1. Secure Communications Interoperability	1-1
1.1.2. SCIP Development	1-1
1.1.3. Edition A Version 2	1-1
1.2. AIM	1-1
CHAPTER 2 SECURE COMMUNICATIONS INTEROPERABILITY PROTOCOL (SCIP)	2-1
2.1. INTRODUCTION	2-1
2.1.1. Background	2-1
2.2. SCIP SPECIFICATIONS	2-1
2.2.1. General Description	2-2
2.3. NATO SCIP PROFILE	2-2
2.3.1. Baseline	2-2
CHAPTER 3 NATO SCIP PROFILE CONFIGURATION MANAGEMENT	3-1
3.1. INTRODUCTION	3-1
3.1.1. Configuration Management Process	3-1
3.1.2. Review	3-1
3.1.4. Roles and Responsibilities	3-1
CHAPTER 4 SCIP MINIMUM INTEROPERABILITY PROFILE (SCIP MIP)	4-1
4.1. SCIP MINIMUM INTEROPERABILITY PROFILE	4-1
ANNEX A SCIP SPECIFICATIONS	A-1
ANNEX B SUPPORTING SCIP DOCUMENTATION	B-1

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1. BACKGROUND

1.1.1. Secure Communications Interoperability. Secure Communications Interoperability is difficult to achieve. Due to proprietary technology and/or national policies, secure systems and devices generally only interoperate with each other over one type of network technology. NATO's ambition is to establish a NATO Networked Enabled Capability (NNEC) that is robust and secure and composed of interconnected individual national networks (following the Federated Mission Networking (FMN) principles). The traditional approaches to provide security, in terms of confidentiality, are not able to provide end-to-end security across a Federation of Networks as they are limited to single or individual networks. NATO has recognized that the current approaches to end-to-end security do not lead to secure interoperability. A standardized approach to security will help to mitigate the identified problems. This is reflected in the NATO Cryptographic Interoperability Strategy (NCIS, AC/322-D(2010)0036, 28 Jun 2010).

1.1.2. SCIP Development. In order to overcome the deficiencies in terms of secure end-to-end interoperability, specifications have been defined that enable secure end-to-end interoperability. The specifications are referred to as: Secure Communications Interoperability Protocol (SCIP). SCIP first edition has been developed by the SCIP International Interoperability Control Working Group (SCIP IICWG). It is emphasized that SCIP consists of a set of interoperability specifications that will need to be implemented in equipment to enable secure communications with other SCIP-enabled equipment. The NATO Secure Voice Strategy (NSVS, AC/322-D(2018)0016) has identified SCIP as the target technology to provide interoperable Secure Voice services within the Alliance.

1.2. AIM

1.2.1. The aim of the NATO SCIP Profile is to define a set of SCIP specifications and supporting documentation that are required to enable and support interoperable secure end-to-end communications services over federated and/or heterogeneous networks.

1.3. EDITION A VERSION 3

1.3.1. This new version provides an update of reference module SCIP-214.6, dedicated to the interoperability with the Tactical Secure Voice Cryptographic Interoperability Specification (TSVCIS). This work is known as the Secure Tactical Communications Interoperability Specification (STaC-IS) Release 1.1 and has been developed by the multinational STaC-IS working group.

1.3.2. This version also introduces a new module SCIP-214.7 as a way to transmit SCIP information encapsulated within V.14 and formatted as ITU V-series modem signaling and the resulting modem samples finally encapsulated within a G.711 codec transmitted over an RTP (or SRTP) IP packet.

1.3.3. Last, the version has also allowed the refresh of all modules versions and dates according to the Communication and Information Services Security Standards (CIS3) Partnership¹ reference baseline, as well as an update of the SCIP supporting documentation references.

¹ A Communication and Information (C&I) Partnership. This is a multinational endeavor where the legal framework and secretariat function is provided by the NATO Communication and Information Agency.

CHAPTER 2

SECURE COMMUNICATIONS INTEROPERABILITY PROTOCOL (SCIP)

2.1. INTRODUCTION

2.1.1. **Background.** The SCIP Programme aims at improving secure end-to-end interoperability across various networks deploying different network technologies (heterogeneous networks). These networks include wireless/cellular (GSM/CDMA), wired (PSTN/ISDN), Circuit and Packet Switched, Military and Commercial/civil networks. In order to improve international interoperability, the initial USA SCIP program was extended to include NATO and NATO nations to participate in a Multi National Working Group (SCIP IICWG) to further develop the SCIP specifications. By adding multinational requirements and developing a common cryptographic specification, SCIP would serve as the common protocol and improve the secure end-to-end communications interoperability.

2.1.2. **Development of SCIP.** The SCIP IICWG has developed SCIP protocols that will help to support NATO's ambitions to ensure secure end-to-end interoperability. The SCIP IICWG has used the USA SCIP specifications as a baseline and has built on from there. USA and European industry efforts to implement the SCIP specifications and products are at various stages of development and implementation. In addition to common modes of operation and common specifications, the protocol is flexible and allows the inclusion of national modes of operation. A minimum level of interoperability is assured as all implementations will have to implement a Minimum Interoperability Profile (MIP, SCIP-221). The MIP is essentially a subset of the SCIP Signaling Plan (SCIP 210) and the SCIP Cryptographic Specifications (SCIP 233).

2.2. SCIP SPECIFICATIONS

2.2.1. **General description.** The available SCIP specifications are currently at a level that equipment can be produced. SCIP implementations already exist and NATO has already procured SCIP equipment albeit that these are national implementations of the SCIP protocol. The ultimate aim is to deploy SCIP using the NATO Specifications. Effectively, the NATO SCIP distinguishes from national implementations through the cryptographic aspects. Through experimentation and testing SCIP Interoperability, using the NATO SCIP Specifications (Annex A), has been demonstrated.

2.2.2. It is emphasized that the extant SCIP Interoperability Specifications address various aspects of SCIP. Apart from the Signaling Plan (SCIP 210) and the Minimum Interoperability Profile (SCIP 221) that are effectively common to all SCIP implementations, SCIP specifications may also address specific capabilities (e.g. SCIP 213, 215, 216) and/or network interfaces (SCIP 214 series). In addition, the SCIP Cryptographic Specifications (SCIP 233 and modules) address various cryptographic

aspects that may or may not be included in all SCIP implementations (e.g. a device may only implement secure MELPe (MIP requirement) and not Secure G.729D). It is recognized that the SCIP specifications will evolve to cater for new technological developments in the cryptographic and networking domain.

2.3. NATO SCIP PROFILE

2.3.1. **Baseline.** The NATO SCIP Profile as contained in Annex A of this document is a baseline of SCIP specifications against which industry can build interoperable equipment. The basic SCIP Specifications are contained in the Signaling Plan (SCIP 210) and in the Cryptographic Specifications (SCIP 233). The original SCIP Cryptographic specifications were originally covered by SCIP 231 and 232². As there was a lot of overlap between the SCIP 231 and 232, these were merged into the SCIP 233 that consists of various Reference modules. Other SCIP Specifications refer to specific applications for SCIP (e.g. IP, PSTN, V.150.1. Gateways). This NATO SCIP profile (AComP-5068) will be covered by STANAG 5068. It provides references to NATO agreed SCIP specifications that can be used in support of the development of technical characteristics for the procurement of relevant Cryptographic Equipment for NATO. Nations are encouraged to use the NATO SCIP Profile for their relevant national programmes.

2.3.2. The NATO SCIP Profile consists of the actual SCIP specifications for use in the development of SCIP enabled equipment. In addition there are supporting documents that help to develop the SCIP Specifications such as architectural documents and technical notes. These documents shall be used in the review and assessment of the NATO SCIP Profile. Other supporting documentation consists of Test Plans and Procedures. An overview of SCIP Supporting Documents is included in Annex B.

² In addition, SCIP 232 was always recognized as an interim specification (2007) as a migration to X.509 Certificate structure was considered the way forward for SCIP.

CHAPTER 3 NATO SCIP PROFILE CONFIGURATION MANAGEMENT**3.1. INTRODUCTION**

3.1.1. Configuration Management Process. The SCIP specifications will evolve over time. Further development of the SCIP specifications will be managed by the CIS3 Partnership SCIP Working Group (WG) Board. Once new versions of the SCIP specifications are developed and agreed upon by the CIS3 Partnership SCIP WG Board, they are offered for inclusion in the NATO SCIP Profile. The updated specifications will be reviewed by the C3B Substructure. Once reviewed and endorsed by the appropriate elements in the C3B Substructure, a revised NATO SCIP Profile reflecting the new versions of the SCIP Specifications will be forwarded to the C3B for approval. Once approved by the C3B, the revised NATO SCIP Profile will become the de-facto NATO SCIP Profile and this AComP-5068 will be amended as appropriate.

3.1.2. Review. The actual review of the SCIP specifications by the C3B Substructure will be conducted through the Communications and Information Systems Capability Panel and the Information Assurance and Cyber Defence Capability Panel (CIS CaP (CaP 1) and IACD CaP (CaP 4) respectively)³.

3.1.3. If observations, comments and/or new requirements emerge during the review and assessment process, these shall be forwarded to the the CIS3 Partnership SCIP WG Board for discussion and resolution, if required.

3.1.4. Roles and Responsibilities. Once reviewed, CaP 1 and CaP 4 will provide a recommendation on the NATO SCIP Profile and subsequent updates to the C3B for approval. Once approved, the NATO SCIP Profile will then serve as the Baseline and contain references to the individual specifications with version numbers and related Engineering Change Proposals (ECPs) when relevant.

3.1.5. The supporting staff shall:

- a. Ensure that the SCIP specifications are made available to the appropriate elements within the C3B;
- b. Maintain the NATO SCIP Profile;
- c. Forward observations and/or comments stemming from the C3B assessment of the SCIP specifications to the the CIS3 Partnership SCIP WG Board;

³ The actual review will happen through CaP 1 – Network and Security CaT and CaP 4 – Crypto CaT. These CaTs may be supported by other experts as required.

- d. Maintain a repository of SCIP specifications;
- e. Maintain a repository of supporting SCIP documentation.
- f. Ensure that supporting SCIP documentation is made available to the appropriate elements within the C3B.

CHAPTER 4 SCIP MINIMUM INTEROPERABILITY PROFILE (SCIP MIP)**4.1. SCIP Minimum Interoperability Profile**

4.1.1. In order to assess whether NATO and National Implementations of the NATO SCIP Profile do conform to the minimum required specifications to ensure interoperability, SCIP Implementations will be tested and evaluated for meeting a minimum level of interoperability. The requirements are reflected in the SCIP Minimum Interoperability Profile (SCIP MIP, SCIP-221). As such, SCIP-221 serves as the NATO Protocol Interoperability Conformance Statement⁴.

4.1.2. The implementation of the features as listed in the MIP ensures that a minimum level of interoperability will be achieved. When implemented correctly, SCIP will as a minimum support one or more of the following applications:

- a. Secure Voice based on MELPe (STANAG 4591) at 2.4. kbits/sec;
- b. Secure Reliable Data Transport with and without Error Extension.

4.1.3. Voice, Data or both may be implemented in equipment. The minimum implementation requirement is listed in the MIP. The MIP assists to validate the SCIP implementations and to assess the level of interoperability between NATO and nations.

⁴ Within SCIP 221, reference is made to SCIP 232. SCIP 232 was and is recognized as an interim specification (2007) as a migration to X.509 Certificate structure was considered the way forward for SCIP. SCIP 221 thus refers to keysets 0x0B and 0x0C as reflected in the former SCIP-232. This is the only interoperable specification as long as a X.509 Certificate structure based Key management System is not available. As soon as a X.509 capable Key Management System is available, SCIP-221 will be updated and refer to the corresponding X.509 based keysets.

INTENTIONALLY BLANK

ANNEX A SCIP SPECIFICATIONS

Specification Reference	Rev.	Title	Date	Remarks
SCIP-210	3.10.	SCIP Signaling Plan	26 Oct 2017	
SCIP-221	3.1	MINIMUM IMPLEMENTATION PROFILE (MIP)	6 Feb 2015	
APPLICATION/NETWORK SPECIFIC SCIP SPECIFICATION				
SCIP-213	1.1	MULTI MEDIA OPTION SPECIFIC MINIMUM ESSENTIAL REQUIREMENTS FOR SECURE COMMUNICATION INTEROPERABILITY PROTOCOL (SCIP) DEVICES	28 Feb 2014	
SCIP-213.1	1.0	GENERIC PACKET DATA OPTION	24 Sep 2010	
SCIP-213.2	1.0	PACKET DATA OPTION PROFILES OPTION	28 Feb 2014	
SCIP-214	1.3	NETWORK-SPECIFIC MINIMUM ESSENTIAL REQUIREMENTS (MER) FOR SECURE COMMUNICATION INTEROPERABILITY PROTOCOL (SCIP) DEVICES	02 May 2014	
SCIP-214.1	1.0.	SECURE COMMUNICATION INTEROPERABILITY PROTOCOL (SCIP) OVER THE PUBLIC SWITCHED TELEPHONE NETWORK (PSTN)	10 June 2008	
SCIP-214.2	1.1	SECURE COMMUNICATION INTEROPERABILITY PROTOCOL (SCIP) OVER REAL TIME TRANSPORT PROTOCOL (RTP)	18 Apr 2014	
SCIP-214.3	1.0	SECURING SIP SIGNALING USE OF TLS WITH SCIP	02 May 2014	
SCIP-214.6	1.1	SECURE TACTICAL COMMUNICATIONS – INTEROPERABILITY SPECIFICATIONS (STAC-IS)	Jan 2020	
SCIP-214.7	1.0	SCIP OVER IP USING ITU-T V-SERIES MODEM PASS-THROUGH WITH G.711	18 Dec 2019	
SCIP-215	2.2	U.S. SECURE COMMUNICATION INTEROPERABILITY PROTOCOL (SCIP) OVER IP IMPLEMENTATION STANDARD AND MINIMUM ESSENTIAL REQUIREMENTS (MER) PUBLICATION	08 Jul 2011	
SCIP-216	2.2.	MINIMUM ESSENTIAL REQUIREMENTS (MER) FOR	08 Jul 2011	

		V.150.1 GATEWAYS PUBLICATION		
CRYPTOGRAPHIC SPECIFICATIONS				
SCIP-233	1.3	SECURE COMMUNICATION INTEROPERABILITY PROTOCOL CRYPTOGRAPHY SPECIFICATION – MAIN MODULE	24 Apr 2019	
SCIP-233.102	1.0	REFERENCE MODULE 102 – NATO ELLIPTIC CURVE (EC) KEY MATERIAL SPECIFICATION	31 Mar 2010	
SCIP-233.104	1.0	REFERENCE MODULE 104 – NATO PRE PLACED KEY (PPK) – KEY MATERIAL FORMAT AND FILL CHECKS SPECIFICATION	31 Mar 2010	
SCIP-233.105	1.0	REFERENCE MODULE 105 – UNIVERSAL ELLIPTIC CURVE (EC) KEY MATERIAL SPECIFICATION	31 Mar 2010	
SCIP-233.106	1.1	REFERENCE MODULE 106 – UNIVERSAL CALL SET-UP ENCRYPTION (CSE) KEY MATERIAL; FORMAT AND FILL SPECIFICATION	06 Aug 2012	ECP 045 Active Baseline
SCIP-233.108	1.0	REFERENCE MODULE 108 – UNIVERSAL MULTIPOINT PRE PLACED KEY (PPK) KEY MATERIAL FORMAT AND FILL SPECIFICATION	31 Mar 2010	
SCIP-233.110	1.0	REFERENCE MODULE 110 – MERCATOR CALL SETUP ENCRYPTION (CSE) KEY MATERIAL FORMAT AND FILL SPECIFICATION	17 Oct 2012	
SCIP-233.114	1.0	REFERENCE MODULE 114 – SECURE TACTICAL COMMUNICATIONS – INTEROPERABILITY SPECIFICATIONS (STAC-IS) APPENDIX E AES-256 PRE- PLACED KEY (PPK) KEY SPECIFICATION	01 July 2018	
SCIP-233.150	1.0	REFERENCE MODULE 150 – UNENCRYPTED KEY FILL SPECIFICATION	31 Mar 2010	
SCIP-233.151	1.0	REFERENCE MODULE 151 – CRC CALCULATIONS SPECIFICATION	31 Mar 2010	
SCIP-233.201	1.0	REFERENCE MODULE 201 – UNIVERSAL CALL SET-UP ENCRYPTION(CSE) SPECIFICATION	31 Mar 2010	
SCIP-233.202	1.0	REFERENCE MODULE 202 – MERCATOR CALL SET-UP ENCRYPTION (CSE) SPECIFICATION	17 Oct 2012	

SCIP-233.302	1.0	REFERENCE MODULE 302 – NATO EC AGREEMENT AND TEK DERIVATION SPECIFICATION	31 Mar 2010	
SCIP-233.303	1.0	REFERENCE MODULE 303 – UNIVERSAL ECMQV KEY AGREEMENT AND TEK DERIVATION SPECIFICATION	31 Mar 2010	
SCIP-233.304	1.0	REFERENCE MODULE 304 – NATO POINT-TO-POINT AND MULTIPOINT PPK PROCESSING SPECIFICATION	31 Mar 2010	
SCIP-233.305	1.0	REFERENCE MODULE 305 – UNIVERSAL MULTIPOINT PPK PROCESSING SPECIFICATION	31 Mar 2010	
SCIP-233.307	1.1	REFERENCE MODULE 307 – ECDH KEY AGREEMENT AND TEK DERIVATION	08 Jul 2011	ECP 037 Active Baseline
SCIP-233.308	1.2	REFERENCE MODULE 308 – MERCATOR ECDH KEY AGREEMENT AND TEK DERIVATION SPECIFICATION	18 Apr 2014	
SCIP-233.350	1.3	REFERENCE MODULE 350 – INTEROPERABLE TERMINAL PRIORITY (TP) COMMUNITY OF INTEREST (COI) SPECIFICATION	26 Oct 2017	
SCIP-233.401	1.3	REFERENCE MODULE 401 – APPLICATION STATE VECTOR PROCESSING SPECIFICATION	08 Oct 2013	
SCIP-233.402	1.0	REFERENCE MODULE 402 – CALL SET-UP ENCRYPTION (CSE) STATE VECTOR PROCESSING SPECIFICATION	31 Mar 2010	
SCIP-233.422	1.0	REFERENCE MODULE 422 – NATO FIXED FILLER GENERATION SPECIFICATION	31 Mar 2010	
SCIP-233.423	1.0	REFERENCE MODULE 423 – UNIVERSAL FIXED FILLER GENERATION SPECIFICATION	31 Mar 2010	
SCIP-233.441	1.2	REFERENCE MODULE 441 – POINT TO POINT CRYPTOGRAPHIC VERIFICATION SPECIFICATION	26 Oct 2017	
SCIP-233.442	1.0	REFERENCE MODULE 442 – MULTIPOINT CRYPTOGRAPHIC VERIFICATION SPECIFICATION	31 Mar 2010	
SCIP-233.443	1.2	REFERENCE MODULE 443 – POINT-TO-POINT CRYPTOGRAPHIC VERIFICATION W/HMAC SPECIFICATION	14 Oct 2014	
SCIP-233.444	1.2	REFERENCE MODULE 444 – POINT-TO-POINT CRYPTOGRAPHIC	14 Oct 2014	

		VERIFICATION W/SIGNATURE VERIFICATION		
SCIP-233.445	1.0	REFERENCE MODULE 445 – MERCATOR POINT-TO-POINT CRYPTOGRAPHIC VERIFICATION W/SIGNATURE VERIFICATION	17 Oct 2012	
SCIP-233.501	1.3	REFERENCE MODULE 501 – SECURE MELP(E) VOICE SPECIFICATION	08 Oct 2013	
SCIP-233.502	1.1	REFERENCE MODULE 502 – SECURE G.729D VOICE SPECIFICATION	08 Oct 2013	
SCIP-233.516	1.1	REFERENCE MODULE 516 – SECURE RELIABLE TRANSPORT (RT) ASYNCHRONOUS DATA SPECIFICATION	08 Oct 2013	
SCIP-233.517	1.1	REFERENCE MODULE 517 – SECURE BEST EFFORT TRANSPORT (BET) ASYNCHRONOUS DATA SPECIFICATION	08 Oct 2013	
SCIP-233.518	1.1	REFERENCE MODULE 518 – SECURE ALMOST FULL BANDWIDTH (AFB) DATA	08 Oct 2013	
SCIP-233.519	1.1	REFERENCE MODULE 519 – SECURE FULL BANDWIDTH (FB) DATA	08 Oct 2013	
SCIP-233.531	1.1	REFERENCE MODULE 531 – SECURE PACKET DATA (PD)	08 Oct 2013	
SCIP-233.546	1.1	REFERENCE MODULE 546 – SECURE DIAL PROCESSING SPECIFICATION	08 Oct 2013	
SCIP-233.547	1.1	REFERENCE MODULE 546 – SECURE MESSAGING PROCESSING SPECIFICATION	08 Oct 2013	
SCIP-233.561	1.0	REFERENCE MODULE 561 – FEISTAL ERROR EXTENSION SPECIFICATION	31 Mar 2010	
SCIP-233.562	1.2	REFERENCE MODULE 562 – GALOIS/COUNTER MODE (GCM) DATA INTEGRITY SPECIFICATION	25 Aug 2014	
SCIP-233.563	1.0	REFERENCE MODULE 563 – MONGOOSE ENCRYPTION ALGORITHM SPECIFICATION	08 Oct 2013	
SCIP-233.601	1.0	REFERENCE MODULE 601 – AES-256 ENCRYPTION ALGORITHM SPECIFICATION	31 Mar 2010	
SCIP-233.603	1.0	REFERENCE MODULE 603 – MEDLEY ENCRYPTION ALGORITHM SPECIFICATION	31 Mar 2010	
SCIP-233.604	1.0	REFERENCE MODULE 604 – MERCATOR ENCRYPTION ALGORITHM SPECIFICATION	17 Oct 2012	

SCIP-233.702	1.0	REFERENCE MODULE 702 – NATO ELLIPTIC CURVE (EC) REKEY PROCESING SPECIFICATION	31 Mar 2010	
--------------	-----	--	-------------	--

INTENTIONALLY BLANK

ANNEX B SUPPORTING SCIP DOCUMENTATION

Document Name	Status/Version	Remarks
NC3A Technical Note 980 – Secure End-to End Communications Scenarios	Final	
NATO Secure Voice Strategy	14 March 2018	AC/322-D(2018)0016
NATO Cryptographic Interoperability Strategy	28 June 2010	AC/322-D(2010)0036

NATO UNCLASSIFIED

AComP-5068(A)(3)

NATO UNCLASSIFIED