NATO STANDARD

AComP-4787

NETWORKING AND INFORMATION INFRASTRUCTURE (NII) INTERNET PROTOCOL (IP) NETWORK ENCRYPTOR – INTEROPERABILITY SPECIFICATION (NINE ISPEC)

Edition A Version 1

JANUARY 2018

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED COMMUNICATION PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

25 January 2018

1. The enclosed Allied Communication Publication AComP-4787, Edition A, Version 1 – NETWORKING AND INFORMATION INFRASTRUCTURE (NII) INTERNET PROTOCOL (IP) NETWORK ENCRYPTOR – INTEROPERABILITY SPECIFICATION (NINE ISPEC), 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 4787.

2. AComP-4787, Edition A, Version 1, is effective upon receipt.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

Dieter Schmaglowski
Deputy Director NSO
Branch Head P&C

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
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

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]

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

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1. BACKGROUND

1.1.1. **NATO Networked Enabled Capability (NNEC)**. The NATO Network Enabled Capability (NNEC) Feasibility Study[1] outlined a vision for the Networked Information Infrastructure (NII) that is needed to support the full range of military operations foreseen in the future. An evolutionary approach to the development of the NII was identified, and one of the critical issues in this approach is the availability of flexible and fully interoperable Internet Protocol (IP) networks. The concepts of NNEC have further matured into federated networks both in the static as well as the deployable domain (Federated Mission Networking). Within federated networks, information needs to be exchanged securely between the constituent parts of the overall network. As the individual networks have predominantly migrated to IP networks, interoperable IP Security (IPsec) devices are a pre-requisite to support this secure information exchange.

1.1.2. **IPsec Standardisation**. To achieve interoperable IPsec within federated networks, it is possible to mandate or recommend a specific IPsec implementation. As this will only benefit one manufacturer a more preferable approach is to develop specifications to which manufacturers can build equipment that is interoperable. These are referred to as Interoperability Specifications (ISpec). These specifications could be either system or equipment specific or be interoperability specifications. In the case of IPsec devices, these ISpec would be equipment specific. Experience has demonstrated that interoperability specifications allow for more flexibility in the design of the systems and equipment.This approach enables manufacturers to use and re-use exsiting designs and developments. The ISpec to develop interoperable IPsec devices for the NII are referred to as NII IP Network Encryptor ISpec or NINE ISpec.

1.2. AIM

1.2.1. The aim of this AComp is to define a set of NINE Interoperability Specifications (NINE ISpec) and supporting documentation that are required to enable and support interoperable IPsec services over federated IP Networks.

1.3. DESCRIPTION NINE ISPEC

1.3.1. The primary purpose of NINE devices is to provide high assurance information confidentiality when transporting information between domains of trust. However, as an integral part of the NII it must also be ensured that NINE devices fully support the information flows and management requirements. This implies that various interfaces

[1] NATO C3 Agency (NC3A) NATO Networked Enabled Capability (NNEC) Feasability Study Version 2.0. October 2005.

will need to be defined to cover the full functionality of NINE devices Figure 1 depicts the interfaces that are part of the NINE.

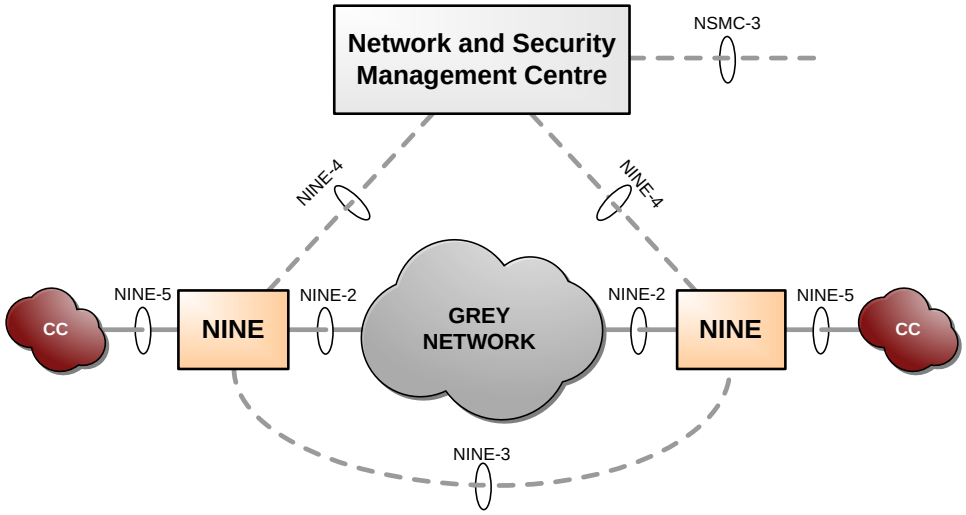

Figure 1: NINE Interfaces

a. Interface NINE-2 is the interface between a NINE device and the grey transport network. This interface is necessary to be able to interoperate with the transport network, whether it is a PCore, a normal network, or a point-to-point link. In a future NII, this transport network will likely be based on Protected Core Networking and will qualify as a PCore, meaning that it provides a trusted, high availability, network.

b. Interface NINE-3 is the logical interface between NINE devices. This interface ensures that NINE devices are able to communicate, negotiate proper security parameters etc. It is used primarily to set up security associations between NINE device peers and to transport packets that have been information confidentiality protected. NINE-3 is necessary to be able to establish security associations between NINE devices regardless of owner and manufacturer.

c. Interface NINE-4 is the logical interface between NINE devices and the Security and Network Management Centre (SNMC). All management traffic, including security management, is handled over NINE-4. NINE-4 is necessary to be able to perform holistic management and to be able to update NINE devices without the need to change the environment and support systems, e.g. key and network management.

d. Interface NINE-5 is the interface between NINE devices and the classified clear-text networks, or coloured clouds (CCs).

e. Interface NSMC-3 is not a NINE interface, but is the interface between network and security management centres. It is listed for completeness over the overall NII

1.3.2. The NINE ISpec specifies the functionality that is needed to achieve interoperability. As such it standardizes the identified NINE interfaces-2, -3 and -5; implementing these functionalities will enable NINE devices to interoperate. Interface NINE 4 will be added to later versions of the NINE ISpec and is closely linked to separate activities that aim to define the Key Management Interoperability.

1.3.3. A nation that is to acquire IP encryption devices must specify the device to their own specification, but should make sure that the device includes all functionality in the NINE ISpec, compliant with the most recent version of the NINE ISpec in order to ensure that:

a. the device is NINE compliant;

b. IPsec interoperability in federated network environments, within a NATO or any other coalition context is established.

INTENTIONALLY BLANK

CHAPTER 2

NETWORK AND INFORMATION INTEROPERABILITY (NII) INTERNET PROTOCOL (IP) NETWORK ENCRYPTOR INTEROPERABILITY SPECIFICATIONS (NINE ISPEC)

2.1. INTRODUCTION

2.1.1. **Background**. The NINE ISpec have been developed to support interoperable IPsec services. After consideration of technical and non-technical criteria, the USA High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specifications have been used as the basis for the development of the NINE ISpec. The NINE ISpec will now serve as a basis and allows manufacturers from different nations to develop and produce interoperable IPsec devices to be used in federated IP network environments such as the Federated Mission Networking (FMN).

2.1.2. **Development of NINE ISpec**. The Space and Naval Warfare Systems Command (SPAWAR) have developed the HAIPE ISpec, that formed the basis for the NINE ISpec. After the HAIPE ISpec was selected by NATO to serve as the basis for the NINE ISpec, interested (NATO-)nations, led by the USA, joined together to develop the NINE ISpec. The working group responsible for the development of the NINE ISpec was the NINE ISpec Working Group (NISWG). The requirements for the NINE ISpec were reflected in the NINE Level of Ambition that served as an overall guidance. Within the NINE level of Ambition, a distinction was made between Version 1 and follow-on versions of the NINE ISpec. Version 1.0.4. of the NINE ISpec was the first set of agreed NINE ISpec. This Version of the NINE ISpec covers the vast majority of the NINE Level of Ambition Version 1. The required time to develop the remaining NINE ISpec to meet the NATO Level of Ambition Version 1, coupled with their impact on the overall performance of the NINE ISpec did not justify it to address these in Version 1 of the NINE ISpec and these will now be addressed in later versions of the NINE ISpec. This approach will allow to have interoperable IPsec devices available to replace existing IPsec devices and support the emerging requirements within an acceptable timeframe.

2.1.3. The follow-on development of the NINE ISpec will be managed through the Multi-National Communication and Information Systems Security Standards Communication and Information Partnership (CIS3 C&IP), supported by the NCI Agency.

2.2. NINE INTEROPERABILITY SPECIFICATIONS (NINE ISPEC)

2.2.1. **General description**. The available NINE ISpec can support the development of IPsec devices that are NINE Compliant and interoperable with each other. The individual NINE ISpec form the NINE ISpec Profile (Annex A) that is adopted by NATO to be used for providing the required confidentiality services within a federated IP-

network. As this NINE ISpec does not contain the specifications of the Network and Security management, manufacturers may implement a proprietary Network and Security Management Interface to manage the NINE devices.

2.2.2. **NINE / NINE ISpec Supporting Information**. The NINE and NINE ISpec are supported by the following sets of Documentation (Annex B) that will be updated as the NINE ISpec evolves:

a. NINE Management Information Base (MIB) to support the common basic management functions of NINE devices. The management functions are based on the Simple Network Management Protocol (SNMP);

b. NINE References (USA and NATO);

c. Internet Engineering Task Force Requests for Comments (IETF RFCs).

CHAPTER 3 NINE ISPEC MAINTENANCE AND CONFIGURATION MANAGEMENT

3.1. BACKGROUND

3.1.1. **Introduction**. As a result of developing, deploying and testing NINE ISpec compatible equipment, changes to the NINE ISpec (Version 1 and follow-on versions) can be expected (e.g. bug fixing, removing ambiguities). This is generally considered to be maintenance of a Standard. In addition, requirements may evolve that require a change or addition to the NINE ISpec. The nations participating in the NINE ISpec development will discuss and agree on the required changes to the NINE ISpec. Whichever changes will occur to the NINE ISpec, these will need to be well documented to ensure continued interoperability; this is generally referred to as: 'Configuration management'.

3.1.2. **Configuration Management**. To ensure and maintain the consistency of the NINE ISpec throughout its lifetime, a Configuration Management Process will be set up. Through the NISWG, a (Draft) Configuration Management Plan was developed[2] . This Plan will serve as the basis for the Configuration Management of the NINE ISpec development, but will be amended, if required, as the development of NINE ISpec will become a joint responsibility of the participating nations through the Multi-National Communication and Information Systems Security Standards Communication and Information Partnership (CIS3 C&IP).

3.2. NATO ADOPTION OF THE NINE ISPEC

3.2.1. **General**. Once new or updated NINE ISpec have been developed and agreed by the nations involved in the NINE ISpec development, these will be offered to NATO in order to be included in this AComP. Updated and/or new specifications will be reviewed by the C3O Substructure. Once reviewed and endorsed by the appropriate elements in the C3O Substructure, a revised AComP-4787, reflecting the new versions of the NINE ISpec, will be forwarded to the C3B for approval. Once approved by the C3B, a new version of the AComP-4787 will be forwarded to the NATO Standardization Office for processing in accordance with the extant Standardization procedures.

3.2.2. **Review**. The review of the NINE IS by the NC3O Substructure will be conducted through the Communications and Information Systems Capability Panel (CIS CaP (CaP 1)) and the Information Assurance and Cyber Defence Capability Panel (IACD CaP (CaP 4)) [3]. If observations, comments and/or new requirements emerge during

[2] (Draft) Configuration Management Plan for Networking and Information Infrastructure Internet Protocol Network Encryption (NINE) (SSCPAC–NINE-CMP V0.1) 28 May 2010

[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.

the review and assessment process, these shall be forwarded to the NISWG or the Multi-National Communication and Information Systems Security Standards Communication and Information Partnership (CIS3 C&IP) for further discussion and resolution, if required.

3.2.3. **Roles and Responsibilities**. Once reviewed, CaP 1 and CaP 4 will provide a recommendation on the NINE ISpec and subsequent updates to the C3B for approval. Once approved, the updated NINE ISpec, then serve as the Baseline and contain references to the individual specifications with version numbers and related Engineering Change Proposals.

3.2.4. The supporting staff[4] shall:

a. Ensure that the NINE ISpec are made available to the appropriate elements within the NC3O;

b. Maintain STANAG 4787 and AComP 4787;

c. Forward observations and/or comments stemming from the NC3O assessment of the NINE ISpec to the NISWG/ Multi-National Communication and Information Systems Security Standards Communication and Information Partnership (CIS3 C&IP);

d. Maintain a repository of NINE ISpec;

e. Maintain a repository of supporting NINE ISpec Documentation.

f. Ensure that supporting NINE ISpec Documentation is made available to the appropriate elements within the NC3O.

[4] The supporting staff will be the NHQC3Sup until the moment the Multi-National Communication and Information Systems Security Standards Communication and Information Partnership (CIS3 C&IP) has been established. Once this Partnership has been established, the NCI Agency will provide the required supporting functions to the development of the NINE ISpec.

CHAPTER 4 NINE ISPEC Minimum Interoperability Requirements (IPMEIR)

.

4.1. NINE ISpec Minimum Interoperability Requirements (MIR)

4.1.1. The NINE ISpec is comprised of the Core and several Optional Extensions. The Core contains a set of ‘Treshold’ (mandatory) requirements, considered Minimum Interoperability Requirements (MIR). NINE Devices must implement the Core to be considered NINE ISpec compliant.

4.1.2. Extensions contain ‘Treshold’ (Mandatory) and ‘Objective’ (Optional) requirements. An Extension is considered to be implemented if all ‘Treshold’ (Mandatory) requirements of that Extension are implemented. Its ‘Objective’ (optional) requirements may be implemented.

INTENTIONALLY BLANK

ANNEX A NINE INTEROPERABILITY SPECIFICATIONS

Networking Information Infrastructure (NII) Internet Protocol Network Encryptor (NINE) Interoperability Specification (ISpec)			
NINE IS Version	Title	Date	Remarks
1.0.4.	Traffic Protection – Suite B Cryptography	16 Feb 2015	
1.0.4.	Traffic Protection - Suite A MEDLEY Cryptography	16 Feb 2015	Classified Specification
1.0.4.	Traffic Protection - Suite A MERCATOR Cryptography	16 Feb 2015	Classified Specification
1.0.4.	Traffic Protection – IKE v2 Suite B Cryptography	16 Feb 2015	
1.0.4.	Traffic Protection - IKEv2 Suite A MEDLEY Cryptography	25 Jun 2015	Classified Specification
1.0.4.	Traffic Protection - IKEv2 Suite A MERCATOR Cryptography	25 Jun 2015	Classified Specification
1.0.4.	Render Useless – Zeroization Net Controller	16 Feb 2015	
1.0.4.	Render Useless – Zeroization Client	16 Feb 2015	
1.0.4.	Remote Provisioning	16 Feb 2015	
1.0.4.	Remote Provisioning - Authority	16 Feb 2015	
1.0.4.	Remote Cryptography – Ignition Key Net Controller	16 Feb 2015	
1.0.4.	Remote Cryptography – Ignition Key Client	16 Feb 2015	
1.0.4.	Remote Configuration and Monitoring	16 Feb 2015	
1.0.4.	Reachability	16 Feb 2015	
1.0.4.	IPsec Minimum Essential Interoperability Requirements	16 Feb 2015	
1.0.4.	Header Compression	16 Feb 2015	
1.0.4.	Generic Discovery Client	16 Feb 2015	
1.0.4.	Gateway	16 Feb 2015	
1.0.4.	Dynamic Multicast Discovery and Keying	16 Feb 2015	

1.0.4.	Core	16 Feb 2015	
1.0.4.	Certificate Revocation List Transfer	16 Feb 2015	
1.0.4.	Bandwidth management	16 Feb 2015	
1.0.4.	Automated SA-IKEv2	16 Feb 2015	

ANNEX B NINE ISPEC SUPPORTING DOCUMENTATION

Networking Information Infrastructure (NII) Internet Protocol Network Encryptor (NINE) Interoperability Specification (IS) – Management Information Base (MIB)			
NINE IS MIB Version	Title	Date	Remarks
1.0.4.	Traffic Protection	17 Feb 2015	
1.0.4.	Textual Conventions	17 Feb 2015	
1.0.4.	RUZ	17 Feb 2015	
1.0.4.	ROHC - Robust Header Compression	17 Feb 2015	
1.0.4.	RCIK	17 Feb 2015	
1.0.4.	Networking	17 Feb 2015	
1.0.4.	Management	17 Feb 2015	
1.0.4.	Key Transfer	17 Feb 2015	
1.0.4.	Key Information	17 Feb 2015	
1.0.4.	Feature Hierarchy	17 Feb 2015	
1.0.4.	DMDK	17 Feb 2015	
1.0.4.	Discovery	17 Feb 2015	
1.0.4.	CRL (Certificate Revocation List) – Transfer	17 Feb 2015	
1.0.4.	Compliance	17 Feb 2015	
1.0.4.	Bandwidth Management	17 Feb 2015	
1.0.4.	MIB (Management Information Base)	17 Feb 2015	
1.0.4.	Assignments	17 Feb 2015	

ANNEX B TO
AComP-4787

Networking Information Infrastructure (NII) Internet Protocol Network Encryptor (NINE) Interoperability Specification (IS) – References

	Title	Date	Remarks
	Suite B Implementers Guide	28 Jul 2009	
	ON716929 48 Bit Electronic Serial Nxxxxxx Standard (ESN) – Rev 1.2.	2 Mar 2007	
	National Security Systems (NSS) Public Key Certificate (PKC) and Certificate Revocation Lists (CRL) Profiles v.1.6.	30 Sep 2013	
	NIST - Mathematical Routines for NIST Prime Curves	5 Apr 2010	
	HAIPE X.509 Requirements V. 2.1.	5 May 2014	
	Electronic Key management System 324 (EKMS 324) – Advanced Encryption Standard (AES)	31 Jul 2008	
	Electronic Key management System 310 (EKMS 310) – Advanced Encryption Standard (AES) Key Wrap Length Indicator and Binding Code Specification	31 Jul 2008	
	Electronic Key management System 308 (EKMS 308) – Data Standard and Delivery Standard Rev. F	16 Apr 2008	
	Electronic Key management System 304 (EKMS 304) – Cyclic Redundancy Check (CRC)-32 Check Word Specification (EKMS Phase 4 Baseline)	18 Jun 2003	
	CACMB Spec 9170		
	CACMB Spec 9160 – Generalized Concatenation Key derivation Function, specified for the use with SHA-384 Rev. B	20 Dec 2005	Draft

	CACMB Spec 9130 – A Key Update Function Based on the AES Key Wrap	10 Jan 2005	
	Authenticated HAIPE IS Foreign Interoperability PPK Specification, Version 3.2	10 Jan 2007	
	EU Suite A Key Wrap Mode of Operation v1.0	June 2010	Classified
	R21-TECH-30-1: MEDLEY Implementation Standard		Classified
	R21-TECH-03-02: An ACCORDION MEDLEY		Classified
	Pre-Placed Key Format for High Assurance IP Encryptor Interoperability Specification	27 July 2005	
	NINE Suite A Elliptic Curve Cryptography		Classified
	The Pseudo-Random Function (PRF) for NINE		
	FIPS 197: Advanced Encryption Standard,	26 Nov 2001	
	FIPS-180-2 Secure Hash Standard,	1 Aug 2002	
	Description of the VEGAS family of Algorithms v. 1.4.	21 Mar 2005	Classified
	VEGAS Specifications for MERCATOR		Classified

Other References			
	Title	Date	Remarks
AC/322(SC/4)N(2008)0042 (AC/322(SC/6)N(2008)0050)	NINE Interoperability Level of Ambition	2 Oct 2008 (23 Sep 2008)	

Internet Engineering Task Force – Request For Comments (IETF RFC)			
IETF RFC	Title	Date	Status
768	User Datagram Protocol	Aug 1980	Internet Standard
791	Internet Protocol	Sep 1981	Internet Standard
792	Internet Control Message Protocol	Sep 1981	Internet Standard
1112	Host extensions for IP multicasting	Aug 1989	Internet Standard
1350	The TFTP Protocol (Revision 2)	Jul 1992	Internet Standard
2080	RIPng for IPv6	Jan 1997	Proposed Standard
2113	IP Router Alert Option	Feb 1997	Proposed Standard
2131	Dynamic Host Configuration Protocol	Mar 1997	Draft Standard
2236	Internet Group Management Protocol, Version 2	Nov 1997	Proposed Standard
2347	TFTP Option Extension	May 1998	Draft Standard
2348	TFTP Blocksize Option	May 1998	Draft Standard
2349	TFTP Timeout Interval and Transfer Size Options	May 1998	Draft Standard
2453	RIP Version 2	Nov 1998	Internet Standard
2460	Internet Protocol, Version 6 (IPv6) Specification	Dec 1998	Draft Standard
2461	Neighbor Discovery for IP Version 6 (IPv6)	Dec 1998	Draft Standard
2462	IPv6 Stateless Address Autoconfiguration	Dec 1998	Draft Standard
2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Dec 1998	Draft Standard
2578	Structure of Management Information Version 2 (SMIv2)	Apr 1999	Internet Standard
2579	Textual Conventions for SMIv2	Apr 1999	Internet Standard
2580	Conformance Statements for SMIv2	Apr 1999	Internet Standard
3014	Notification Log MIB	Nov 2000	Proposed Standard
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	Jul 2003	Proposed Standard
3376	Internet Group Management Protocol, Version 3	Oct 2002	Proposed Standard
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	Dec 2002	Internet Standard
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	Dec 2002	Internet Standard

3413	Simple Network Management Protocol (SNMP) Applications	Dec 2002	Internet Standard
3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	Dec 2002	Internet Standard
3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	Dec 2002	Internet Standard
3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)	Dec 2002	Informational
3417	Transport Mappings for the Simple Network Management Protocol (SNMP)	Dec 2002	Informational
3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	Dec 2002	Internet Standard
3513	Internet Protocol Version 6 (IPv6) Addressing Architecture	Apr 2003	Proposed Standard
3602	The AES-CBC Cipher Algorithm and Its Use with IPsec	Sep 2003	Proposed Standard
3706	A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers	Feb 2004	Informational
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	Jun 2004	Proposed Standard
3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	Jun 2004	Proposed Standard
3948	UDP Encapsulation of IPsec ESP Packets	Jan 2005	Proposed Standard
4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	Jun 2005	Proposed Standard
4301	Security Architecture for the Internet Protocol	Dec 2005	Proposed Standard
4306	Internet Key Exchange (IKEv2) Protocol	Dec 2005	Proposed Standard
4506	XDR: External Data Representation Standard	May 2006	Internet Standard
4718	IKEv2 Clarifications and Implementation Guidelines	Oct 2006	Informational
4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)	Jan 2007	Proposed Standard

4868	sing HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec	May 2007	Proposed Standard
4869	Suite B Cryptographic Suites for IPsec	May 2007	Informational
5225	RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite	Apr 2008	Proposed Standard
5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	May 2008	Proposed Standard
5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol	Aug 2008	Proposed Standard
5406	Guidelines for Specifying the Use of IPsec Version 2	Feb 2009	Informational
5759	Suite B Certificate and Certificate Revocation List (CRL) Profile	Jan 2010	Informational
5795	The RObust Header Compression (ROHC) Framework	Mar 2010	Proposed Standard
5857	IKEv2 Extensions to Support Robust Header Compression over IPsec	May 2010	Proposed Standard
5903	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2	Jun 2010	Informational
5996	Internet Key Exchange Protocol Version 2 (IKEv2)	Sep 2010	Proposed Standard
7630	HMAC-SHA-2 Authentication Protocols for the User-based Security Model USM for SNMP v. 3.0		

NINE was based on the referenced RFCs some of which were only used for informational purposes

INTENTIONALLY BLANK

AComP-4787(A)(1)