

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
Section 4 Information Assurance.....	4-1
4.1. Introduction.....	4-1
4.1.1 Product Configuration Considerations.....	4-1
4.2. Requirements	4-2
4.2.1 The [Alarm] Tag: Generation of Alarms	4-2
4.2.2 Product Category Definitions	4-2
4.2.3 User Roles.....	4-3
4.2.4 Ancillary Equipment.....	4-5
4.2.5 VVoIP Authentication	4-7
4.2.6 VVoIP Authorization.....	4-9
4.2.7 Public Key Infrastructure.....	4-10
4.2.8 Integrity.....	4-16
4.2.9 Confidentiality	4-17
4.2.10 Non-Repudiation.....	4-28

LIST OF TABLES

<u>TABLE</u>		<u>PAGE</u>
Table 4.2-1.	Acronyms and Appliances Specifying Type of Component.....	4-2

SECTION 4

INFORMATION ASSURANCE

4.1. INTRODUCTION

This section defines the interoperability focused Information Assurance (IA) requirements for Unified Capabilities (UC) products. These products include but are not limited to Softswitches (SSs), Session Controllers (SCs), Session Border Controllers (SBCs), and End Instruments (EIs). While Voice and Video over Internet Protocol (VVoIP) IA remains a key focus area, over time this section has been expanded to incorporate the general IA requirements for additional UC Approved Products List (APL) products. This section of the Unified Capabilities Requirements (UCR) now incorporates the general information assurance requirements for a number of UC APL “Security Devices,” generally considered to be “Information Assurance Products” in accordance with Department of Defense (DOD) Directive (DODD) 8500.1. These requirements include network-based Firewalls (FWs), Intrusion Prevention Systems (IPs), Virtual Private Network (VPN) servers, and Network Access Controllers (NACs), for example. More information on Security Devices can be found in Section 13, Security Devices, which specifies the “security-device-unique” functional requirements for these products.

A number of requirements have been removed from this UCR section in order to minimize the number of requirements that overlap with the requirements already found in Defense Information Systems Agency (DISA) Facility Security Office (FSO) Security Technical Implementation Guides (STIGs). The STIGs now serve as the primary baseline for purely IA-focused requirements, and this UCR section focuses on those requirements that impact interoperability from an IA standpoint. Since both the UCR and STIGs are utilized during testing, the intent is to minimize redundancy in information assurance test procedures and reports.

4.1.1 Product Configuration Considerations

In many cases, a system is composed of multiple appliances. For example, typically an SC is composed of a Call Connection Agent (CCA), a media server, a configuration server, a voicemail server, and other servers. Because of the wide variation in vendor products, it is impossible to break out the requirements for each component of a system and the reader should apply the higher level requirements to that component unless specifically stated. For example, the SC requirements apply to a media server within the SC system, even though this relationship is not directly stated. On the other hand, Media Gateway (MG) and EI requirements are called out separately; therefore, the SC requirements would not apply to these devices.

During information assurance testing at approval DOD laboratories, UC APL products are tested against the UCR requirements in this section and information assurance requirements found in other sections of the UCR (e.g., 5, 13), as applicable, in addition to the STIGs. For all products not directly addressed within Section 4 or other UCR sections from an IA perspective, IA testing for the product will include testing against all applicable STIGs.

The requirement key words (i.e., REQUIRED, CONDITIONAL) are defined elsewhere in this UCR. Failure to satisfy a requirement in this section will result in a Technical Deficiency Report (TDR), which differs from past versions of this section in which the requirements were adjudicated as UCR CAT I, II, or III findings in the IA Test Report.

Finally, the requirements that follow do not include all administrative requirements (nontechnical) associated with policy and the STIGs. For instance, if someone is required to document something administratively (e.g., waiver, pilot request) as part of site accreditation, that requirement is not included.

4.2. REQUIREMENTS

4.2.1 The [Alarm] Tag: Generation of Alarms

When the [Alarm] tag appears after a requirement’s applicability statement (e.g., Required and Conditional), this indicates that the product must support, at a minimum, the capability to perform the following functions in addition to complying with the specified requirement:

1. Generate an alarm to the Network Management System (NMS) based on the alarmable actions identified in the requirement and using the configured alarm transmission mechanism [e.g., Simple Network Management Protocol (SNMP), syslog, email].
2. Record an entry in the product’s system and audit logs indicating that the event occurred.

This tag is intended to facilitate rapid identification of all those requirements that result in alarm conditions by automated requirement management tools.

4.2.2 Product Category Definitions

[Table 4.2-1](#), Acronyms and Appliances Specifying Type of Component, shows the acronyms and appliances that represent a specific UC APL product.

Table 4.2-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
EI	End Instrument [Including Multipoint Conference Units (MCUs) and other devices that provide EI-equivalent functionality on their respective interfaces]
FW	Data Firewall
IPS	Intrusion Detection/Prevention System
LS	Local Area Network (LAN) Switch
MG	Media Gateway
NAC	Network Access Controller
R	Router
RSF	Real-Time Services (RTS) Stateful Firewall

ACRONYM	APPLIANCES
SBC	Session Border Controller
SC	Session Controller
SD	Security Device [generic, overarching category which encompasses all devices addressed in Section 8 including FW, IPS, VPN, NAC, Wireless Intrusion Detection System (WIDS)]
SS	Softswitch
UEI	UC Session Initiation Protocol (SIP) Video End Instrument (including MCUs and other devices that provide UEI-equivalent functionality on their respective interfaces)
VPN	Virtual Private Network Concentrator and Termination
WIDS	Wireless Intrusion Detection System

4.2.3 User Roles

IA-000010 [Required: SS, SC] [Former ID: 5.4.6.2.1.3-1.a] The product shall be capable of having at least five types of user roles: a system security administrator (e.g., auditor), a system administrator, an application administrator, a privileged application user, and an application user.

IA-000020 [Required: R, LS, SBC, RSF, MG] [Former ID: 5.4.6.2.1.3-1.b] The product shall be capable of having at least three types of user roles: a system security administrator (e.g., auditor), a system administrator, and an application administrator.

IA-000030 [Required: EI, UEI] [Former ID: 5.4.6.2.1.3-1.c] The product shall be capable of supporting at least three types of user roles: a system administrator, a privileged application user, and an application user.

NOTE: The product demonstrates the ability to support a privileged application user by being able to dial precedence digits to signal the SC the precedence of the session.

IA-000040 [Required: EI, UEI] [Former ID: 5.4.6.2.1.3-1.d] The product shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.

IA-000050 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.3-1.h.3] The product shall be capable of providing a mechanism for the appropriate administrator (not a user in the User role) to perform the following functions:

- a. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.3-1.h.3.c]**
Monitor the activities of a specific terminal, port, or network address of the system in real time.
- b. **[Required:., SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.3-1.h.3.q]**
Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.

- c. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.3-1.h.3.bb]**
Provide a capability to monitor the system resources and their availabilities.

IA-000060 [Required: SD] [Former ID: 5.4.6.2.1.3-1.r] The product shall support at least four roles: Cryptographic Administrator (CAAdmin), Audit Administrator (AAdmin), System Administrator, User.

NOTE: The CAAdmin and AAdmin roles are defined in National Information Assurance Partnership (NIAP) publications.

- a. **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1]** The ability to perform the following functions shall be restricted to the System Administrator role:
- (1) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1.a]** Modify security functions.
 - (2) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1.b]** Enable or disable security alarm functions.
 - (3) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1.c]** Enable or disable the Internet Control Message Protocol (ICMP) and destination unreachable notification on external interfaces [in an Internet protocol (IP)-based network], or other appropriate network connectivity tool (for a non-IP-based network).
 - (4) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1.d]** Determine the administrator-specified period for any policy.
 - (5) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1.e]** Set the time/date used for timestamps.
 - (6) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1.f]** Query, modify, delete, and/or create the information flow policy rule set.
 - (7) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.1.h]** Revoke security attributes associated with the users, information flow policy rule set, and services available to unauthenticated users within the security device.
- b. **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.2]** The ability to enable, disable, determine, and/or modify the functions of the security audit or the security audit Analysis shall be restricted to the AAdmin role.
- c. **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.3]** The ability to perform the following functions shall be restricted to the CAAdmin role:
- (1) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.3.a]** Enable and/or disable the cryptographic functions.
 - (2) **[Required: SD] [Former ID: 5.4.6.2.1.3-1.r.3.c]** Modify the cryptographic security data.

4.2.4 Ancillary Equipment

IA-000070 [Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.a] Products that use external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with (IAW) Request for Change (RFC) 3588.

- a. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.a.1]** Systems that act as Diameter agents shall be capable of being configured as proxy agents.
 - (1) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.a.1.a]** Systems that act as proxy agents shall maintain session state.
- b. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.a.2]** All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.
- c. **[Conditional: SS, SC, MG, SBC, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.a.3]** All Diameter implementations shall provide transport of its messages IAW the transport profile described in RFC 3539.
- d. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.a.4]** Products that use the Extensible Authentication Protocol (EAP) within Diameter shall do so IAW RFC 4072.

IA-000080 [Required: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.b] Products shall support the capability to use the Remote Authentication Dial In User Service (RADIUS) IAW RFC 2865 to provide AAA services.

NOTE: Unlike previous UCR revisions where RADIUS was a Conditional requirement, RADIUS is now a capability that is Required when supporting AAA services.

- a. **[Required: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.b.1]** Products that use the EAP within RADIUS shall do so IAW RFC 3579.
- b. **[Required: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.b.2]** If the products support RADIUS based accounting, then the system shall do so IAW RFC 2866.

IA-000090 [Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.c] Products that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so IAW the TACACS+ Protocol Specification 1.78 (or later).

NOTE: The intent is to use the most current TACACS+ specification.

IA-000100 [Conditional: EI, UEI] [Former ID: 5.4.6.2.1.4-1.d] Products that use external address assignment services provided by the Dynamic Host Configuration Protocol (DHCP) shall do so IAW RFC 2131.

NOTE: An external address assignment service is a service that extends beyond the boundary of the system.

- a. **[Conditional: EI, UEI] [Former ID: 5.4.6.2.1.4-1.d.1]** Products that act as DHCP clients upon receipt of a new IP address shall probe [e.g., with Address Resolution Protocol (ARP)] the network with the newly received address to ensure the address is not already in use.

NOTE: The actions to take if a duplicate address is detected are found in RFC 2131.

- b. **[Conditional: EI, UEI] [Former ID: 5.4.6.2.1.4-1.d.2]** Products that act as DHCP clients upon receipt of a new IP address shall broadcast an ARP reply to announce the client's new IP address and clear outdated ARP cache entries in hosts on the client's subnet.

IA-000110 [Conditional: R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.e] Products that use external AAA services provided by port based network access control mechanisms shall do so IAW Institute of Electrical and Electronics Engineers (IEEE) 802.1X-2010 in combination with Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) support, at a minimum, plus any other desired secure EAP types [e.g., EAP-Tunneled TLS (TTLS)].

- a. **[Conditional: R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.1.4-1.e.1]** Products that use external EAP services provided by EAP shall do so IAW RFC 3748 and its RFC extensions.

IA-000120 [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.4-1.f] Products that use external syslog services shall support the capability to do so IAW RFC 3164.

- a. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.4-1.f.1]** Products that support syslog over User Datagram Protocol (UDP) IAW RFC 3164 shall use UDP port 514 for the source port of the sender when using UDP for transport.
- b. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.4-1.f.3]** If the product supports syslog, then the product shall support the capability to generate syslog messages that have all the parts of the syslog packet as described in Section 4.1 of RFC 3164.
 - (1) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.4-1.f.3.a]** If the originally formed message has a **TIMESTAMP** in the **HEADER** part, then it shall support the capability to specify this field's value in the local time of the device

within its time zone and support the ability to specify this field's value in Greenwich Mean Time (GMT).

(2) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.4-1.f.3.b]**

If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address.

(3) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.4-1.f.3.c]**

If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message.

- c. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, FW, IPS, VPN, NAC] [Former ID: 5.4.6.2.1.4-1.f.4]** If products use Transmission Control Protocol (TCP) for the delivery of syslog events, then the system shall support the capability to do so IAW the Read and Write (RAW) profile defined in RFC 3195.

IA-000130 [Required: SBC] [Former ID: 5.4.6.2.1.4-2] The product shall either support an onboard VVoIP Intrusion Detection System (IDS)/IPS capability that can monitor all VVoIP signaling and media traffic in decrypted form, or support the capability to present all signaling and bearer traffic to an external VVoIP IDS/IPS in a secure manner.

- a. **[Required: SBC] [Former ID: 5.4.6.2.1.4-2.a] [Alarm]** The VVoIP IDS/IPS threat detection capabilities shall be IAW the VVoIP IDS/IPS functional requirements specified in Section 13, Security Devices. The product shall support the capability to generate and transmit an alarm to the NMS when these threats are identified.
- b. **[Conditional: SBC] [Former ID: 5.4.6.2.1.4-2.c]** If the product provides the capability to transmit decrypted VVoIP media and signaling to an external IDS/IPS platform, then this interface shall use publicly accessible specifications and standards.

NOTE: The intent of this requirement is to ensure that third party IDS/IPS vendors have the information necessary to create an interface that can accept and process the received VVoIP information.

4.2.5 VVoIP Authentication

IA-000140 [Required: SC] [Former ID: 5.4.6.2.1.5-1.a.3] The product shall be capable of authenticating the EI using TLS (or its equivalent) (Threshold) and/or with Public Key Infrastructure (PKI) certificates issued from a DOD-approved PKI.

NOTE: This assumes the EI is served directly by the appliance.

IA-000150 [Required: SC] [Former ID: 5.4.6.2.1.5-1.a.4] The product shall be capable of authenticating the UEI using TLS with PKI certificates issued from a DOD-approved PKI.

IA-000160 [Required: EI] [Former ID: 5.4.6.2.1.5-1.a.5] The product shall be capable of authenticating the SC using TLS (or its equivalent) (Threshold) and/or with PKI certificates issued from a DOD-approved PKI.

IA-000170 [Required: UEI] [Former ID: 5.4.6.2.1.5-1.a.6] The product shall be capable of authenticating the SC using TLS with PKI certificates issued from a DOD-approved PKI.

IA-000180 [Required: EI, UEI] [Former ID: 5.4.6.2.1.5-1.g] The product shall be capable of allowing users to place ROUTINE precedence calls without authenticating.

IA-000190 [Required: EI, UEI] [Former ID: 5.4.6.2.1.5-1.g.1] The product shall be capable of allowing users to place emergency calls without authenticating.

IA-000200 [Required: EI, UEI] [Former ID: 5.4.6.2.1.5-1.h] The product shall only allow authenticated users to access the product for services above the ROUTINE precedence.

- a. **[Conditional: SC, EI, UEI] [Former ID: 5.4.6.2.1.5-1.h.1]** If the product uses SIP or UC SIP, then the system shall, at a minimum, support the use of SIP digest authentication as specified in RFC 3261 when authenticating users. The product may support the ability to authenticate users via PKI certificates when authenticating user credentials to the SC via the EI or the UEI using proprietary mechanisms.

NOTE: The SC is responsible for the authentication decisions. The method for authenticating a user with their PKI certificate is a vendor decision due to the immaturity of the current standards. Vendors may choose to implement user authentication using PKI certificates as described in RFC 3261 or as described in RFC 3893.

- (1) **[Required: SC, EI, UEI] [Former ID: 5.4.6.2.1.5-1.h.1.a]** The product shall use the procedures and algorithms specified in RFC 3261, Section 22.4, to execute SIP digest authentication for user authentication. The user ID entered by the user shall be used for the value of the “username” field and the Personal Identification Number (PIN) entered by the user shall be used as the value for “secret” in the digest calculation.

- (2) **[Required: EI, UEI] [Former ID: 5.4.6.2.1.5-1.h.1.b]** The device shall support the capability to provide audible and/or visible notification to the user, which, in a human understandable manner, prompts them to enter their assigned User-ID and PIN when a precedence level above ROUTINE is requested.

- b. **[Required: SC, EI, UEI] [Former ID: 5.4.6.2.1.5-1.h.2]** The user authentication mechanism shall be software enabled or disabled.

NOTE: In certain deployments, the user does not have the time to input authentication credentials and the EI or UEI is located in a secure environment where credentials are not necessary due to the mission. By default this capability will be disabled to allow users to place calls without authenticating.

- (1) [**Conditional: EI, UEI, (Softphone)**] [**Former ID: 5.4.6.2.1.5-1.h.2.a**] If the product is a softphone, then the product shall support the capability to provide user authentication by presenting the user credentials extracted from the Common Access Card (CAC) or other DOD PKI Project Management Office (PMO)-approved PKI token to the SC.

NOTE: The mechanism for UEIs and EIs to authenticate the User CAC or approved token credentials is permitted to occur via proprietary means. However, authentication of users via User ID and PIN authentication has been standardized for UEIs in this UCR.

IA-000210 [**Required: SS, SC, MG, SBC, AEI**] [**Former ID: 5.4.6.2.1.6-1.j.3**] The product shall adhere to the requirements in RFC 5922, Section 7.2, “Comparing SIP Identities,” when comparing the domains extracted from X.509v3 certificates with UC SIP identities contained in signaling messages.

IA-000220 [**Conditional: SS, SC**] [**Former ID: 5.4.6.2.1.6-1.j.5**] If the system supports AEIs that use the sip.instance media feature tag (RFC 5626), then the system shall ensure that the identity claimed in the AEI's X.509 certificate Subject Common Name presented during TLS session establishment maps to the UC SIP Address of Record (AOR) and sip.instance values specified in UC SIP signaling messages.

NOTE: This requirement is meant to ensure that the identity claimed by a registering AEI in UC SIP is authorized based on its presented X.509 certificate.

4.2.6 VVoIP Authorization

IA-000230 [**Required: R, LS, SBC, RSF**] [**Former ID: 5.4.6.2.1.7-1.d.1**] The product shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, Differentiated Services Code Point (DSCP), and protocol identifier (“6 tuple”).

IA-000240 [**Required: SBC, RSF**] [**Former ID: 5.4.6.2.1.7-1.d.1.a**] The product shall have the capability of opening and closing “gates/pinholes” (i.e., packet filtering based on the “6 tuple”) based on the information contained within the Session Description Protocol (SDP) body of the UC SIP messages.

IA-000250 [**Required: SBC, RSF**] [**Former ID: 5.4.6.2.1.7-1.d.1.a.i**] The product shall have the capability to close a “gate/pinhole” based on a configurable media inactivity timer and issue a BYE message to upstream and downstream UC SIP signaling appliances (lost BYE scenario).

NOTE: The inactivity timer is based on the inactivity of the media stream.

IA-000260 [**Required: SBC, RSF**] [**Former ID: 5.4.6.2.1.7-1.d.1.a.i.A**] The default media inactivity value for closing a session and issuing BYE messages shall be 15 minutes.

IA-000270 [Required: R, SBC, RSF] [Former ID: 5.4.6.2.1.7-1.d.1.b] The product shall have the capability of permitting the configuration of filters that will permit or deny IP packets on the basis of the values of the packet's source address, destination address, protocol, source port, and destination port in the packets header. These filters shall have the capability of using any one value, all values, or any combination of values. Filters using source ports and destination ports shall have the capability to be configured to use ranges of values defined by the operators (1) equal to, (2) greater than, (3) less than, (4) greater than or equal to and (5) less than or equal to.

IA-000280 [Required: R, LS] [Former ID: 5.4.6.2.1.7-1.d.2.a] The product shall be capable of supporting a minimum of five distinct VLANs for VVoIP.

IA-000290 [Required: SBC] [Former ID: 5.4.6.2.1.7-1.d.3.a] The product shall be capable of using Network Address Translation (NAT) and Network Address Port Translation (NAPT) on all VVoIP enclave-to-Wide Area Network (WAN) connections.

IA-000300 [Required: R, SBC, RSF] [Former ID: 5.4.6.2.1.7-1.d.3.a.i] The product shall have the capability to deploy using private address space IAW RFC 1918.

IA-000310 [Required: SBC] [Former ID: 5.4.6.2.1.7-1.d.3.a.ii] The SBC shall be an UC SIP intermediary in all WAN signaling sessions.

IA-000320 [Required: SBC] [Former ID: 5.4.6.2.1.7-1.d.3.a.ii.A] To enable the application of NAT and NAPT, the SBC shall be able to inspect and modify the SDP body (i.e., the SDP "c=" and the "m=" lines) of the corresponding UC SIP message.

IA-000330 [Conditional: SBC] [Former ID: 5.4.6.2.1.7-1.d.3.a.iii] If the system supports H.323 video sessions, then the SBC shall be capable of supporting H.323 NAT and NAPT.

IA-000340 [Conditional: R, LS, EI, UEI] [Former ID: 5.4.6.2.1.7-1.d.5.a] If DHCP is used, then the product shall be capable of using 802.1X in combination with a secure EAP type (defined within this UCR and the STIGs) residing on the authentication server and within the operating system or application software of the EI and UEI to authenticate to the LAN.

IA-000350 [Required: RSF] [Former ID: 5.4.6.2.1.7-1.d.6] The product shall be capable of being configured to ensure that VVoIP and non-VVoIP traffic between their respective VLANs is filtered and controlled so that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.

IA-000360 [Required: SBC, RSF] [Former ID: 5.4.6.2.1.7-1.d.7.a] The product FWs deployed at the boundaries of the VVoIP enclave shall have the capability to use stateful packet inspection.

4.2.7 Public Key Infrastructure

IA-000370 [Required: SS, SC, MG, SBC, RSF, R, UEI, NAC, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.a.1] The product shall be capable of generating asymmetric keys whose length is at least 2048 for Remote Secure Access (RSA).

IA-000380 [Required: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.a.2] The product shall be capable of generating symmetric keys whose length is at least 128 bits.

IA-000390 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.b] The product shall be capable of storing key pairs and their related certificates.

IA-000400 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.b.2.e] The product shall operate with DOD-approved trust points [e.g., public keys and the associated certificates the relying party deems as reliable and trustworthy, typically root certification authorities (CAs)].

NOTE: Trust points are further defined in Appendix A of this UCR, Definitions, Abbreviations and Acronyms, and References.

- a. **[Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.b.2.e.i]** The product shall authenticate individual certificates up to a trusted DOD-approved CA (intermediate or root).
- b. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, LS, EI, SD] [Former ID: 5.4.6.2.1.6-1.b.2.e.ii]** If a trust point is not established, then the product shall authenticate individual certificates from the issuer specified on the individual certificate up to the root CA.

IA-000410 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.d] The product shall be capable of supporting end entity server and device certificates and populating all certificate fields IAW methods described in the “DOD PKI Functional Interface Specification.”

IA-000420 [Required: SS, SC, MG, SBC, RSF, R, UEI, NAC, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.e.1] The product shall be capable of using the Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), Hypertext Transfer Protocol (HTTP), or HTTP Secure (HTTPS) as appropriate when communicating with DOD-approved PKIs.

IA-000430 [Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.a] If Certificate Revocation Lists (CRLs) are used, then the product shall be capable of using either the date and time specified in the next update field in the CRL or using a configurable parameter to define the period associated with updating the CRLs.

IA-000440 [Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.b] If CRLs are used, then the product shall be capable of obtaining the CRL from the CRL Distribution Point (CDP) extension of the certificate in question. The product shall be able to process HTTP pointers in the CDP field whereas the ability to process HTTPS and LDAP pointers is Objective.

NOTE: This requirement does not prevent the product from supporting the ability to use manually configured, local CDPs which differ from the CDP provided in the certificate.

IA-000450 [Conditional: SS, SC, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.c] If Online Certificate Status Protocol (OCSP) is used, then the product shall support the capability to use both the Digital Trunk Module (DTM), whereby the OCSP responder's signing certificates are signed by DOD approved PKI CAs, and the OCSP Trusted Responder model, where the OCSP responder uses a self-signed certificate to sign OCSP responses, IAW DOD PKI PMO guidance.

NOTE: The OCSP responder's DTM certificate is appended to every OCSP response sent from the DOD PKI OCSP responders. Products should expect these certificates to change regularly (approximately every 30 days).

NOTE: RFC 2560 describes both the Trust Responder and Delegated Trust (termed "Authorized Responder" within RFC 2560) models. Though DOD PKI-specific implementation details can only be found in DOD PKI PMO publications.

IA-000460 [Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.d] If OCSP is used, then the OCSP responder shall be contacted based on the following information:

- a. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.d.i]** The OCSP responder preconfigured in the application or toolkit; and
- b. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.d.ii]** The OCSP responder location identified in the OCSP field of the Authority Information Access (AIA) extension of the certificate in question.
- c. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.d.iii]** If both of the above are available, then the product shall be configurable to provide preference for one over the other.
- d. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.e.3.d.iv]** The product should (not shall) be configurable to provide preferences or a preconfigured OCSP responder based on the Issuer DN.

IA-000470 [Conditional: EI] [Former ID: 5.4.6.2.1.6-1.e.4] If the EI is PKI enabled, then the EI shall support a mechanism for verifying the status of an SC certificate using a Certificate Trust List (CTL), CRLs, or an online status check (OCSP in the case of the DOD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OCSP requirements specified previously and later in this section.

IA-000480 [Conditional: SC] [Former ID: 5.4.6.2.1.6-1.e.5] If the EI is PKI enabled, then the SC shall verify the status of an EI certificate using the CTL, CRLs, or an online status check (OCSP in the case of the DOD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OCSP requirements specified previously and later in this section.

IA-000490 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.e.6] The product shall support all of the applicable requirements in the latest DOD Public Key Encryption (PKE) Application Requirements specification published by the DOD PKI PMO.

NOTE: At the time of this UCR's writing, the "DOD Class 3 Public Key Infrastructure Public Key-Enabled Application Requirements" document from July 13, 2000 is the latest version of this document.

IA-000500 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.f.1] The product shall be capable of producing Secure Hash Algorithm (SHA) digests of messages to support verification of DOD PKI signed objects.

IA-000510 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.f.1.a] The product shall support the capability to verify certificates, CRLs, OCSP responses, or any other signed data produced by a DOD approved PKI using RSA in conjunction with the SHA-256 algorithm.

NOTE: During the migration to SHA-256, certificate chains may contain a mix of certificates signed using either SHA-1 or SHA-256 within the same chain.

IA-000520 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.1.6-1.f.3] The product shall log when a session is rejected due to a revoked certificate.

IA-000530 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.g] The product shall be capable of supporting the development of a certificate path and be able to process the path.

NOTE: The path development process produces a sequence of certificates that connect a given end-entity certificate to a trust point. The process terminates when either the path tracks from a trust point to an end entity or a problem occurs that prohibits validation of the path.

- a. **[Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.g.3]** The path process shall fail when a problem that prohibits the validation of a path occurs.

- b. **[Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.g.5]** The product shall be capable of ensuring that the intended use of the certificate is consistent with the DOD-approved PKI extensions.
- c. **[Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.g.6]** The product shall be capable of ensuring that the key usage extension in the end entity certificate is set properly.
 - (1) **[Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.g.6.a]** The product shall be capable of ensuring that the digital signature bit is set for authentication uses.
 - (2) **[Required: SS, SC, MG, SBC, RSF, R, UEI, NAC, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.g.6.b]** The product shall be capable of ensuring that the non-repudiation bit is set for non-repudiation uses.

IA-000540 [Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI] [Former ID: 5.4.6.2.1.6-1.g.4.a.i] [Alarm] During VVoIP session establishment, if the product uses an online status check to validate a certificate and the product cannot contact the online status check responder (OSCR) (in the case of the DOD PKI, this will be an RFC 2560 OCSP responder) and backup OSCs, the product will establish the VVoIP session (e.g., shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions. This requirement is not applicable to scenarios related to non-VVoIP-session related functions such as logging on to administrative interfaces. The intent of this requirement is to prevent phone or video calls from being denied due to connectivity issues with the OCSP responder.

IA-000550 [Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI] [Former ID: 5.4.6.2.1.6-1.g.4.a.ii] [Alarm] During VVoIP session establishment, if the product uses CRLs to validate a certificate and the product cannot reach the CDP or any backup CDPs, the product will continue the process (e.g. shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions (see the note on the preceding requirement).

IA-000560 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.h] Periodically, the system shall examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions based on updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired.

NOTE: The system must not terminate VVoIP sessions simply because of a failure to retrieve the latest CRL or perform an online status check.

- a. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.h.1]** If the system supports manual loading of a CRL or CTLs configured by an administrator, then the system shall check all ongoing sessions as soon as updates to the internally stored CRL or trust lists occur.
- b. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.h.2]** If the system supports automated retrieval of a CRL from a CDP, then the system shall immediately check the certificates and trust chains associated with all ongoing sessions against the newly retrieved CRL.
 - (1) **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.h.2.b]** If the system supports automated retrieval of a CRL from a CDP, then the system shall support the ability to configure the interval in which the CRL is retrieved periodically.
- c. **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.h.3]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DOD PKI), then the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked.
 - (1) **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.h.3.a]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DOD PKI), by default, for each session, then the device shall query the online status check responder every 24 hours for as long as the session remains active.
 - (2) **[Conditional: SS, SC, MG, SBC, RSF, R, UEI, EI, LS, SD] [Former ID: 5.4.6.2.1.6-1.h.3.b]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DOD PKI), then the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.

IA-000570 [Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.i] [Alarm] The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.

NOTE: Since EIs and UEIs are not expected to have direct access to the NMS, the SC, Multifunction Softswitch (MFSS), or SS is expected to generate this alert to the NMS on behalf of any subtended EIs or UEIs. However, EIs and UEIs should also alert their users via the EI or UEI user interface when certificates are nearing expiration.

NOTE: There is no expectation for vendors to develop a proprietary protocol for this purpose. It is sufficient for an MFSS, SS, or SC to inspect the certificate of a served

EI or UEI during registration time and periodically thereafter for the duration of the signaling session. Some products may also store the certificate associated with their subscribing EIs and UEIs so as to enable this check to be performed even when the EIs and UEIs are offline.

- a. **[Required: SS, SC, MG, SBC, RSF, R, UEI, LS, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.i.1] [Alarm]** By default, the system shall be capable of sending this alert 60 days before the expiration of the installed credentials, which cannot be renewed automatically. This alert should be repeated periodically on a weekly or biweekly basis by default.

IA-000580 [Required: SS, SC, MG, SBC, RSF, AEI, EI, SD; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.j] The product shall support the capability to verify that the identity claimed in an X.509v3 certificate Subject Common Name, used to establish an authenticated and secure channel, correctly maps to the identity claimed in signaling messages transmitted within the same secure channel.

NOTE: At this time the identity claimed in an X.509v3 certificate Subject Common Name may be a FQDN, IPv4, or IPv6 address.

IA-000590 [Required: SS, SC, MG, SBC, EI, AEI; Conditional: EI] [Former ID: 5.4.6.2.1.6-1.j.2] The product shall support the capability to examine the identity claimed by the X.509v3 Subject Common Name field and compare it to the identity claimed within signaling messages regardless of whether the claimed identity contains an FQDN, IPv4 address, or IPv6 address.

IA-000600 [Required: SS, SC, MG, SBC, RSF, AEI, EI] [Former ID: 5.4.6.2.1.6-1.j.4] The product shall support the capability to statically map the FQDNs contained in X.509v3 certificate Subject Common Names to IP addresses via a configurable lookup table.

NOTE: Use of DNS to map X.509v3 Subject Common name fields to IP addresses may be optionally supported in addition to this requirement. However, using DNS in this manner is not required because all MILDEP sites will not be configured to populate certificates with only DNS associated X.509 Subject Common Name FQDNs.

4.2.8 Integrity

IA-000610 [Required: SS, SC, SBC, RSF, UEI; Conditional: EI] [Former ID: 5.4.6.2.2-1.a.1] The product shall be capable of using TLS for providing integrity of UC SIP messages.

NOTE: The condition for the EI is the support of UC SIP.

- a. **[Required: SS, SC, SBC, RSF, UEI; Conditional: EI] [Former ID: 5.4.6.2.2-1.a.1.a]** The product shall be capable of using Hash-Based Message Authentication Code (HMAC)-SHA1-160 with 160 bit keys.

IA-000620 [Conditional: SS, SC, EI, UEI] [Former ID: 5.4.6.2.2-1.a.2] If the product uses H.323, then the product shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMAC-SHA1-96 with 160 bit keys.

IA-000630 [Required: EI, UEI, MG, SS] [Former ID: 5.4.6.2.2-1.h] The product shall be capable of providing data integrity of the Secure Real-Time Transport Protocol (SRTP) bearer (transport) packets.

- a. **[Required: EI, UEI, MG, SS] [Former ID: 5.4.6.2.2-1.h.1]** The product shall be capable of using HMAC-SHA1-32 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTP packets.
- b. **[Required: EI, UEI, MG, SS] [Former ID: 5.4.6.2.2-1.h.2]** The product shall be capable of using HMAC-SHA1-80 for the authentication tag with 160 bit key length as the default integrity mechanism for Secure Real-Time Transport Control Protocol (SRTCP).

NOTE: The ability to process received SRTCP messages is optional, but the capability to transmit SRTCP messages is required.

IA-000640 [Conditional: SS, SC, MG, SD] [Former ID: 5.4.6.2.2-1.m] If the product uses IP Security (IPSec), then the product shall be capable of using HMAC-SHA (class value 2) as the default Internet Key Exchange (IKE) integrity mechanism as defined in RFC 2409.

IA-000650 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.2-1.n] The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160-bit key length by default.

IA-000660 [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.2-1.o] If the product uses SSHv2, then the product shall use HMAC-SHA1-96 with 160 bit key length for data integrity.

IA-000670 [Conditional: SS, SC, MG, SBC, RSF, EI, UEI, SD] [Former ID: 5.4.6.2.2-1.p] If the product uses TLS, then the product shall be capable of using TLS [Secure Socket Layer (SSL) v3.1 or higher] in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for the session packets.

4.2.9 Confidentiality

IA-000680 [Required: EI, UEI, MG] [Former ID: 5.4.6.2.3-1.b] The product shall be capable of providing confidentiality for media streams using SRTP with either the AES_CM_128 encryption algorithm as the default.

- a. **[Required: SS, SC, MG, EI, UEI] [Former ID: 5.4.6.2.3-1.b.2]** The product shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages IAW RFC 4568.

- b. **[Required: SS, SC, MG, EI, UEI] [Former ID: 5.4.6.2.3-1.b.3]** The product shall be capable of distributing the Master Key and the Salt Key in concatenated form.
- c. **[Required: EI, UEI, MG] [Former ID: 5.4.6.2.3-1.b.4]** The product shall use a Master Key of 128 bits to support 128-bit Advanced Encryption Standard (AES) encryption.

NOTE: This implies that the Master Salt Key may be null.

- d. **[Required: EI, UEI, MG] [Former ID: 5.4.6.2.3-1.b.5]** The Master Key and a random Master Salt Key shall be supported for SRTP sessions.
- e. **[Required: SS, SC, SBC, MG, UEI, EI] [Former ID: 5.4.6.2-11]** When the system assigns the port numbers to a session, the system shall assign the SRTP port ranges within a configurable range between 2048 and 65535 with the default between 16384 to 32764.

IA-000690 [Conditional: SS, SC, MG, EI, UEI] [Former ID: 5.4.6.2.3-1.c.1] If H.323, Media Gateway Control Protocol (MGCP), or H.248 (MEGACO) is used, then the product shall be capable of using IPSec to provide confidentiality.

- a. **[Conditional: SS, SC, MG] [Former ID: 5.4.6.2.3-1.c.1.a]** If the product uses H.248 (MEGACO), then the product shall be capable of distributing the SRTP Master Key and Salt Key in the SDP "k =" crypto field when using H.248.15.
- b. **[Conditional: SS, SC, MG, EI, UEI] [Former ID: 5.4.6.2.3-1.c.1.b]** If H.323 is used, then the product shall be capable of distributing the SRTP Master Key and Salt Key in H.235 using the H235Key as described in H.235.0 and H.235.8.

IA-000700 [Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c] If IPSec is used, then the product shall be capable of using IKE for IPSec key distribution:

- a. **[Required: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c.i]** The product shall be capable of using IKE version 1.
- b. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c.iii]** If IPSec is used, then the product shall be capable of using the digital signature authentication mode with X.509 certificates during Phase I of the Internet Security Association and Key Management Protocol (ISAKMP) negotiation for authentication.
- c. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c.iv]** If IPSec is used, then the product shall be capable of using the Quick Mode as the default Phase II Security Association mechanism for the IPSec service.
- d. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c.v]** If IPSec is used, then the product shall be capable of using and interpreting certificate requests for Public-Key Cryptography Standard #7 (PKCS#7) wrapped certificates as a request for the whole path of certificates.

- e. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c.vi]** If IPsec is used, then the product shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.
- f. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c.vii]** If IPsec is used, then the product shall be capable of using Oakley Groups 1, 2, and 2048, as a minimum.
- g. **[Conditional: SS, SC, MG, FW, IPS, VPN, NAC] [Former ID: 5.4.6.2.3-1.k]** If the product uses IPsec, then the system shall be capable of using AES_128_CBC as the default encryption algorithm. The system shall be capable of supporting 3DES-CBC (class value 5) for backwards compatibility with previous UCR revisions.
- h. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.c.1.c.vi.A]** If IPsec is used, then the product shall only support the following erroneous messages associated with a certificate request:
 - (1) Invalid Key.
 - (2) Invalid ID.
 - (3) Invalid certificate encoding.
 - (4) Invalid certificate.
 - (5) Certificate type unsupported.
 - (6) Invalid CA.
 - (7) Invalid hash.
 - (8) Authentication failed.
 - (9) Invalid signature.
 - (10) Certificate unavailable.

IA-000710 [Required: SS, SC, MG, SBC, RSF, UEI] [Former ID: 5.4.6.2.3-1.c.2] The product shall be capable of using TLS (dual path method) to provide confidentiality for the UC SIP as described in RFC 3261.

NOTE: Upon receipt of an INVITE over a TLS-established session, an SC shall respond to the INVITE (and any subsequent requests received over that TLS path) using this TLS session. If the SC originates an INVITE or request, then it shall establish a separate and unique TLS session, and the SC shall expect to receive a response to its request over this new TLS session. Two TLS sessions are established for communications between the SC and the SBC, MFSS and SBC, SC and SC, SC to UEI via RSF, or SBC and SBC. Since the UEI is required to support the dual path method, it has to act as both a SIP client and server and must support both TLS client and server functionality. Due to the proprietary nature of line side IP solutions

implemented by EIs, EI vendors may support TLS reuse or the dual path method described in this requirement for line side implementations. The details associated with the reuse method are described in <http://tools.ietf.org/html/rfc5923>.

- a. **[Required: SS, SC, MG, SBC, RSF, UEI; Conditional: EI] [Former ID: 5.4.6.2.3-1.c.2.a]** The underlying protocol for UC SIP shall be the TCP.
- b. **[Required: SS, SC, MG, SBC, RSF, UEI; Conditional: EI] [Former ID: 5.4.6.2.3-1.c.2.b]** The product shall be capable of using as its default cipher suite TLS_RSA_WITH_AES_128_CBC_SHA.
- c. **[Required: SS, SC, MG, SBC, RSF, UEI; Conditional: EI] [Former ID: 5.4.6.2.3-1.c.2.c]** The product shall be capable of using a default of no compression for UC SIP messages.
- d. **[Required: SS, SC, MG, SBC, RSF, UEI; Conditional: EI] [Former ID: 5.4.6.2.3-1.c.2.d]** The product shall be capable of exchanging UC SIP TLS messages in a single exchange or multiple exchanges.
- e. **[Required: SS, SC, MG, SBC, RSF, UEI; Conditional: EI] [Former ID: 5.4.6.2.3-1.c.2.e]** The product shall be capable of distributing the SRTP Master Key and Salt Key in the UC SIP message using the SDP crypto= field.

NOTE: EI condition is whether it supports UC SIP.

- f. **[Conditional: SS, SC, MG, SBC, RSF, UEI, EI] [Former ID: 5.4.6.2.3-1.c.2.f]** If TLS session resumption is used, then a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with Network Management (NM)-related sessions.

- (1) **[Conditional: SS, SC, MG, SBC, RSF, UEI, EI] [Former ID: 5.4.6.2.3-1.c.2.f.i]** If TLS session resumption is used, then the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process (e.g. a full handshake) is 1 hour.

- g. **[Conditional: SS, SC, EI, SBC, RSF, UEI] [Former ID: 5.4.6.2.3-1.c.2.g]** If UC SIP is used, then the product shall transmit only packets that are secured with TLS and use port 5061.

NOTE: The products may use other signaling protocols for interfacing to e.g. MGs, EIs.

- h. **[Required: SS, SC, EI, SBC, RSF, UEI] [Former ID: 5.4.6.2.3-1.c.2.h]** The product shall reject all received UC SIP packets associated with port 5061 that are not secured with TLS.

NOTE: This ensures that the product does not process UDP, Stream Control Transmission Protocol (SCTP), and TCP SIP packets that are not secured using a combination of TLS and TCP.

- i. **[Required: SS, SC, EI, SBC, RSF, UEI] [Former ID: 5.4.6.2.3-1.c.2.i]** The product shall only accept and process UC SIP packets that arrive on port 5061.

NOTE: The product should discard UC SIP packets that arrive on a different port.

- j. **[Required: RSF] [Former ID: 5.4.6.2.3-1.c.2.j]** The product shall support both the reuse and dual path TLS methods.

NOTE: This is required of an RSF since it has to support TLS sessions between the SC and UEI and Proprietary IP Voice EIs (PEIs). The UEI uses the dual path method and PEIs have the option of using the reuse method.

IA-000720 [Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.f] If the product uses TLS, then the product shall do so in a secure manner as defined by the following subtended requirements.

- a. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, UEI, SD] [Former ID: 5.4.6.2.3-1.f.1]** If the product uses TLS, then the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA as its default cipher suite.
- b. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.f.2]** If the product uses TLS, then the system shall be capable of using a default of no compression.
- c. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.f.3]** If the product uses TLS, then the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges.
- d. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.f.4]** If TLS session resumption is used, then a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with NM-related sessions.

- (1) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.f.4.a]** If TLS session resumption is used, then the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process is 1 hour.
- e. **[Required: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.f.5]** If the product supports SSL/TLS renegotiation, then the product shall support the capability to disable this feature or the product shall support RFC 5746.

NOTE: Supporting RFC 5746 includes providing a configurable option to terminate a TLS session if the peer does not support the “renegotiation_info” extension.

IA-000730 [Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g] If the product uses Secure Shell (SSH), then the system shall do so in a secure manner as defined by the following subtended requirements.

NOTE: An EI’s remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

a. **[Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.1]** If the product uses SSH, then the system shall be capable of supporting the RSA 2,048-bit key algorithm and the Diffie-Hellman 2,048 bit key algorithm.

(1) **[Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.a]** If the product uses SSH, then a client shall close the session if it receives a request to initiate an SSH session whose version is less than 2.0.

NOTE: Closing the session may be either a default behavior or a configurable option. If this is a configurable option, then the conditions of fielding should clearly specify that this option must be configured.

(2) **[Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.b]** If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data received or every 60 minutes, whichever comes sooner.

(3) **[Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.c]** If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data transmitted or every 60 minutes, whichever comes sooner.

(4) **[Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.f]** If the product uses SSH, then the SSH sessions shall minimally support the following encryption algorithms defined in RFC 4253 and RFC 4344:

- AES128-CTR
- AES128-CBC (for backwards compatibility with older UCR versions).

(a) **[Conditional: SS, SC, MG, SBC, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.f.i]** If the product uses SSH, then the SSH sessions shall use as the default (most preferred) encryption algorithm AES128-CTR.

(5) **[Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.g]** If the product uses SSH, then the SSH sessions shall use TCP as the underlying protocol.

(6) [Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.h] If the product uses SSH, then it shall be capable of processing packets with uncompressed payload lengths up to 32,768 bytes or shall be configurable to specify that value; also, this length shall be the default value. This does not preclude the system from automatically sizing the Maximum Transmission Unit (MTU) if it is less than 32,768.

(a) [Conditional: SS, SC, SBC, RSF, EI, UEI, R, LS, MG, SD] [Former ID: 5.4.6.2.3-1.g.2.h.i] If the product uses SSH, then the SSH packets shall have a maximum packet size of 35,000 bytes or shall be configurable to that value; also, this length shall be the default value.

NOTE: The 35,000 bytes includes the packet_length, padding_length, payload, random padding, and MAC.

(b) [Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.h.ii] If the product uses SSH, then the product shall discard SSH packets that exceed the maximum packet size to avoid denial of service (DoS) attacks or buffer overflow attacks.

(c) [Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.h.iii] If the product uses SSH, then the SSH packets shall use random bytes if packet padding is required.

(7) [Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.i] If the product uses SSH, then the system shall treat all SSH-encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.

(8) [Conditional: SS, SC, MG, SBC, RSF, EI, UEI, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.2.j] If the product uses SSH, then the system shall be capable of setting Diffie-Hellman-Group14-SHA1 as the preferred key exchange mechanism for SSH.

b. [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3] The use of SSH is [Conditional], however, if the product supports the use of SSH in conjunction with X.509v3 certificates (the SSH implementation is DOD PKE) the product shall conform to the subtended requirements.

NOTE: The EIs and UEIs are excluded from this requirement since remote management of the system is disabled after initial installation.

(1) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.b] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH server shall support the capability to use an X.509v3 certificate provided by a DOD-approved PKI.

- (a) [Conditional: SS, SC, MG, SBC, RSF, LS, R, SD] [Former ID: 5.4.6.2.3-1.g.3.b.i] If the product uses SSH with X.509v3 certificates, then the SSH Server function shall support, at a minimum, the “x509v3-ssh-rsa” and "x509v3-rsa2048-sha256” key types as defined in RFC 6187
 - (b) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.b.ii] If the product uses SSH with X.509v3 certificates, then the SSH Server function shall support the capability to, in a configurable manner, specify the highest preferred key type advertised during the SSH_MSG_KEXINIT message exchange.
 - (c) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.b.iii] If the product uses SSH with X.509v3 certificates, then the SSH server function shall support the capability to deny SSH sessions when the session fails to negotiate a configured set of preferred key types.
- (2) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.c] If the product uses SSH with X.509v3 certificates, then the SSH client shall support the capability to use an X.509v3 certificate provided by a DOD-approved PKI.
- (a) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.c.i] If the product uses SSH and if the SSH client has a CAC (or equivalent) reader, then the SSH client may use the X.509v3 certificate on the user’s CAC to establish the encrypted session.
 - (b) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.c.ii] If the product uses SSH and if the client has a CAC (or equivalent) reader and also has its own PKI certificate from a DOD-approved PKI, then the client may use either its certificate or the certificate on the user’s CAC to establish the encrypted sessions.
 - (c) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.c.iii] If the product uses SSH with X.509v3 certificates, then the SSH client shall support, at a minimum, the “x509v3-ssh-rsa” and "x509v3-rsa2048-sha256” key types as defined in RFC 6187.
- (3) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.d] If the product uses SSH with X.509v3 certificates, then the SSH server shall validate the DOD-approved PKI certificate supplied by the SSH client IAW the specifications in PKI Section 4.2.7, Public Key Infrastructure, of this document.
- (4) [Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.e] If the product uses SSH with X.509v3 certificates, then the SSH client shall validate the SSH server’s DOD PKI certificate IAW the specifications in PKI Section 4.2.7, Public Key Infrastructure, of this document.

- (5) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.f]** If the product uses SSH with X.509v3 certificates, then the SSH server shall certify and validate the SSH client's DOD-approved PKI certificate before establishing an encrypted session.

NOTE: The certification and validation consists of determining that the client's certificate has not expired and has not been revoked. The server shall not establish an encrypted session with a client whose certificate has expired or been revoked.

- (6) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.g]** If the product uses SSH with X.509v3 certificates, then the SSH client shall certify and validate the SSH server's DOD-approved PKI certificate before establishing an encrypted session.
- (7) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.h]** If the product uses SSH with X.509v3 certificates, then the system shall disconnect a session if the PKI certificate validation has not been completed within a configurable period. The default shall be 10 minutes.
- (8) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.i]** If the product uses SSH with X.509v3 certificates, then the SSH server shall disconnect if the number of failed validation attempts for a single session exceeds a configurable parameter and the default shall be three attempts.
- (9) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.g.3.a]** If the product uses SSH with X.509v3 certificates, then the system shall support the capability to use X.509v3 certificates issued by a DOD-approved PKI to establish the encrypted sessions.

IA-000740 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h] The product shall be capable of using SNMPv3 for all SNMP sessions.

NOTE: If the product is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, then any findings associated with this requirement may be downgraded. In addition, if the product has developed a migration plan to implement Version 3, then any findings associated with this requirement may be further downgraded.

- a. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.1]** The security level for SNMPv3 in the DOD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. The product shall set snmpSecurityLevel=authPriv as the default security level used during initial configuration.
- b. **[Required: SS, SC, MG, RSF, R, LS, SBC, SD] [Former ID: 5.4.6.2.3-1.h.2]** The SNMPv3 implementation shall be capable of allowing an appropriate administrator to

manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.

- c. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.3]** The security model for SNMPv3 shall be the User-Based Security Model – snmpSecurityModel =3.
 - (1) **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.3.a]** If the product receives response messages, then the product shall conduct a timeliness check on the SNMPv3 message.
 - (2) **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.3.b]** An SNMPv3 engine shall perform time synchronization using authenticated messages.
- d. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.4]** The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3.
- e. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.5]** The product shall support the capability to use Data Encryption Standard-Cipher Block Chaining (DES-CBC) (usmDESPrivProtocol) with a 16 octet (128 bit) input key, as specified in RFC 3414, as an encryption cipher for SNMPv3.
 - (1) **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.5.a]** The product shall support the capability to use the CFB-AES128 encryption cipher usmAesCfb128PrivProtocol for SNMPv3 as defined in RFC 3826 and specify this as the default encryption cipher for SNMPv3.
- f. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.6]** If the product receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.
- g. **[Conditional: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.7]** If the product receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class Protocol Data Unit (PDU) for which there is no outstanding Confirmed Class PDU.
- h. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.8]** When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window.
- i. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.9]** An SNMPv3 Command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window.
- j. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.10]** When sending state altering messages to a managed authoritative SNMPv3 engine, a Command

Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.

- k. **[Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.h.11]** The product using SNMPv3 shall implement the key-localization mechanism.

IA-000750 [Conditional: SS, SC, MG, SBC, RSF, R, LS, UEI, EI, SD] [Former ID: 5.4.6.2.3-1.d] If the product uses web browsers or web servers, then the product web browsers and web servers shall be capable of supporting TLS (SSLv3.1) or higher for confidentiality.

IA-000760 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.3-1.e] The product shall be capable of using SSHv2 or TLS 1.0 (SSLv3.1) or higher for remote configuration of appliances.

NOTE: The EIs and UEIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

IA-000770 [Conditional: SS, SC, MG] [Former ID: 5.4.6.2.3-1.i] If the product uses different signaling protocols (i.e., H.323 and UC SIP), then the system shall be capable of translating or transferring the bearer keys between different signaling protocols.

IA-000780 [Conditional: SS, SC, MG, EI, UEI] [Former ID: 5.4.6.2.3-1.n] If the product is the originating party and receives a 181 message indicating that the call is being forwarded, then, upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a rekeying.

NOTE: The rekeying is designed to prevent the "forwarding party" from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session, then the forwarding party would be able to eavesdrop on the forwarded session. SCs, and SS may act as a B2BUA for an EI or an UEI and so would originate the UC SIP session on behalf of the EI or UEI.

IA-000790 [Conditional: EI, UEI] [Former ID: 5.4.6.2.3-1.o] If the EI or UEI acts as a bridge or a MCU, then it shall establish a unique key for each EI or UEI connection.

IA-000800 [Conditional: SBC] [Former ID: 5.4.6.2.3-1.p] If the product transmits decrypted VVoIP signaling and/or bearer traffic to an external IDS/IPS, then confidentiality for the decrypted signaling and media traffic shall be ensured using cryptographic protection, where the strength of the cryptographic protocol/algorithms used is greater than or equal to the TLS and SRTP cryptographic profiles defined in this document.

4.2.10 Non-Repudiation

IA-000810 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.4-1.b.3] The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).

IA-000820 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.4-1.b.4] Only the System Security Administrator and System Administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s)

IA-000830 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.4-1.b.12] The product/system shall be able to generate a human understandable presentation of any audit data stored in the audit trail.

IA-000840 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] [Former ID: 5.4.6.2.4-1.b.13] The product shall locally store (queue) audit log/event data when communication with the management station is unavailable and transmit the queued data when network connectivity is restored.

NOTE: In the case of protocols that use unreliable delivery, such as syslog over UDP, use of mechanisms at lower Open System Interconnect (OSI) layers (e.g. ICMP, OSI Layer 1 and 2 mechanisms) must be used to detect such connectivity issues.