



National Security
Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

**MOBILE ACCESS
CAPABILITY PACKAGE
VERSION 1.8**



Mobile Access Capability Package



Version 1.8



Mobile Access Capability Package



March 2016

This Commercial Solutions for Classified (CSfC) Capability Package (CP) describes how to protect classified data (including Voice and Video) in Mobile Access Solutions transiting Wired Networks, Domestic Cellular Networks, and Trusted Wireless Networks to include Government Private Cellular Networks and Government Private Wi-Fi networks.

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Mobile Access Capability Package (CP) release for Public Comment	0.8	November 3, 2014	<ul style="list-style-type: none"> Initial release of CSfC Mobile Access guidance for public comment. Incorporates End User Device (EUD) Solution Designs from VPN version 3.0 CP. Incorporates content from Mobile Security Guide version 2.3.
Commercial Solutions for Classified (CSfC) Mobile Access CP	1.0	April 2, 2015	<ul style="list-style-type: none"> Removed "Non-MDF Validated" EUD type Removed EUD design utilizing two VPN Gateways Removed option to utilize separate computing platform with VPN Client installed to provide Outer layer of encryption Changed restrictions on control plane traffic Added Tactical Solution Implementation Appendix Added requirements for End User Device Added requirements for Retransmission Device
Commercial Solutions for Classified (CSfC) Mobile Access CP	1.1		<ul style="list-style-type: none"> Minor update incorporating customer feedback Corrected language in requirement MA-CR-9 and made consistent with the MA CP Compliance Matrix



Mobile Access Capability Package



Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Mobile Access Capability Package (CP) release for Public Comment	1.8	March 2016	<ul style="list-style-type: none">• Added support for Multiple Security Levels• Removed Option to terminate Inner tunnel in the Enterprise/Red Network• Updated Continuous Monitoring architecture and requirements• Added support for EUDs with Dedicated Outer VPN with wireless connectivity to computing device• Relocated Threat Section to associated Risk Assessment document• Update Key Management sections IAW CNSS AM 02-15• Temporarily removed Test Section; updated Test Section will be introduced in MA CP v 2.0



Mobile Access Capability Package



TABLE OF CONTENTS

1	Introduction	9
2	Purpose and Use	9
3	Legal Disclaimer	10
4	Description of the Mobile Access Solution	10
4.1	Networks.....	13
4.1.1	Red Network	13
4.1.2	Gray Network.....	13
4.1.3	Black Network.....	14
4.1.4	Data, Management, and Control Plane Traffic	17
4.2	High-Level Design.....	18
4.2.1	End User Devices.....	19
4.2.2	Independent Site.....	21
4.2.3	Multiple Sites	23
4.2.4	Multiple Security Levels	24
4.3	Rationale for Layered Encryption	25
4.4	Authentication	26
4.5	Other Protocols.....	27
4.6	Availability.....	27
5	Infrastructure Components	27
5.1	Outer Firewall	28
5.2	Outer VPN Gateway	28
5.3	Gray Firewall	29
5.4	Inner Firewall	30
5.5	Gray Management Services	30
5.5.1	Gray Administration Workstation.....	30
5.5.2	Gray Security Information and Event Management (SIEM)	30
5.5.3	Gray Authentication Server.....	31
5.6	Inner Encryption Components.....	31
5.6.1	Inner VPN Gateway.....	32



Mobile Access Capability Package



5.6.2	Inner TLS-Protected Server	32
5.6.3	Inner SRTP Endpoint	33
5.7	Red Management Services.....	33
5.7.1	Red Administration Workstations.....	33
5.7.2	Red Security Information and Event Management (SIEM).....	33
5.8	Public Key Infrastructure Components	34
5.8.1	Outer Certification Authorities	34
5.8.2	Gray Network Certificate Revocation Status Services	34
5.8.3	Inner Certification Authorities	35
5.8.4	Red Network Certificate Revocation Status Services.....	35
6	End User Device Components.....	36
6.1	Outer VPN Component	36
6.1.1	Dedicated Outer VPN.....	36
6.1.2	Outer VPN Client	37
6.2	VPN EUD.....	37
6.3	TLS EUD	38
6.3.1	TLS Client.....	38
6.3.2	SRTP Client	39
7	Mobile Access Configuration and Management.....	39
7.1	Solution Infrastructure Component Provisioning	39
7.2	EUD Provisioning.....	40
7.3	Administration of Mobile Access Components.....	40
7.4	EUDs for Different Classification Domains.....	42
8	Continuous Monitoring.....	42
8.1	Monitoring Points	42
8.2	Log Data	44
8.3	Network Flow Data	45
8.4	Change Detection.....	45
8.5	Collection	45
8.6	Correlation	46



Mobile Access Capability Package



9	Key Management	46
9.1	Distribution Of Certificate Revocation Lists	50
9.2	Remote Rekey of EUD Certificates	51
9.3	WPA2 Key and Certificate Management	52
10	Requirements Overview	52
10.1	Capabilities	52
10.2	Threshold and Objective Requirements	53
10.3	Requirements Designators	54
11	Requirements for Selecting Components	56
12	Configuration Requirements	61
12.1	Overall Solution Requirements	61
12.2	Configuration Requirements for All VPN Components	63
12.3	Configuration Requirements For Inner and Outer VPN Components	66
12.4	Inner VPN Components	67
12.5	Outer VPN Components	68
12.6	Multiple Security Level Requirements	69
12.7	TLS-Protected Server & SRTP Endpoint Requirements	70
12.8	Retransmission Device requirements	72
12.9	Wireless Connectivity to Dedicated Outer VPN	74
12.10	End User Devices Requirements	76
12.11	Port Filtering Requirements for Solution Components	81
12.12	Configuration Change Detection Requirements	83
12.13	Device Management Requirements	84
12.14	Continuous Monitoring Requirements	86
12.15	Auditing Requirements	88
12.16	Key Management Requirements	91
12.16.1	General Requirements	91
12.16.2	Certificate Issuance Requirements	93
12.16.3	Certificate Renewal and Rekey Requirements	95
12.16.4	Certificate Revocation and CDP Requirements	95



Mobile Access Capability Package



12.16.5	Pre-Shared Key (PSK) Requirements.....	97
13	Requirements for Solution Operation, Maintenance, and Handling.....	97
13.1	Requirements for the Use and Handling of Solutions	97
13.2	Requirements for Incident Reporting	100
14	Role-Based Personnel Requirements.....	103
15	Information to Support The AO	105
15.1	Solution Testing	106
15.2	Risk Assessment.....	107
15.3	Registration of Solutions.....	108
16	Testing Requirements	108
	Appendix A. Glossary of Terms	109
	Appendix B. Acronyms	112
	Appendix C. References	115
	Appendix D. End User Device Implementation Notes	117
	Tactical Solution implementations	122

TABLE OF FIGURES

Figure 1.	Overview of Mobile Access Solution.....	11
Figure 2.	Acceptable Black Transport Networks.....	16
Figure 3.	EUD Solution Designs	20
Figure 4.	EUDs Connected to Independent Site.....	21
Figure 5.	Multiple Mobile Access Solution Infrastructures supporting EUDs.....	23
Figure 6.	Mobile Access Solution Supporting Multiple Security Levels	24
Figure 7.	MA Solution Continuous Monitoring Points.....	43

LIST OF TABLES

Table 1.	Overview of Mobile Access CP Terminology.....	11
Table 2.	Acceptable Black Transport Networks	15
Table 3.	Certificate Authority Deployment Options	48
Table 4.	Capability Designators.....	53
Table 5.	Requirement Digraphs	54



Mobile Access Capability Package



Table 6. Product Selection Requirements.....	56
Table 7. Overall Solution Requirements	61
Table 8. Approved Commercial Algorithms (IPsec) for up to Top Secret	63
Table 9. Approved Commercial Algorithms (TLS) for up to Top Secret	64
Table 10. Approved Commercial Algorithms for a Dedicated Outer VPN with Wireless Connectivity	65
Table 11. Approved Commercial Algorithms for up to Top Secret	65
Table 12. Configuration Requirements for Inner and Outer VPN Components	66
Table 13. Inner VPN Components Requirements	67
Table 14. Outer VPN Components Requirements	68
Table 15. Multiple Security Level Requirements	69
Table 16. TLS-Protected Server & SRTP Endpoint Requirements	70
Table 17. Requirements for Retransmission Device	72
Table 18. Requirements for Wireless Connectivity to Dedicated Outer VPN.....	75
Table 19. Requirements for End User Devices.....	76
Table 20. Port Filtering Requirements for Solution Components.....	81
Table 21. Configuration Change Detection Requirements	83
Table 22. Requirements for Device Management	84
Table 23. Continuous Monitoring Requirements	86
Table 24. Auditing Requirements	88
Table 25. PKI General Requirements	91
Table 26. Certificate Issuance Requirements	93
Table 27. Certificate Renewal and Rekey Requirements.....	95
Table 28. Requirements for Certificate Revocation and CDPs.....	95
Table 29. Requirements for the Use and Handling of Solutions.....	98
Table 30. Incident Reporting Requirements	101
Table 31. Role-Based Personnel Requirements.....	104
Table 32. Test Requirements	107



Mobile Access Capability Package



1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency (NSA) Information Assurance Directorate (IAD) publishes Capability Packages (CPs) to provide configurations that empower IAD customers to implement secure solutions using independent, layered Commercial Off-the-Shelf (COTS) products. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and/or Integrators.

IAD is delivering this CSfC Mobile Access (MA) CP to meet the demand for mobile data in transit solutions (including Voice and Video) using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. MA CP Version 1.8 takes lessons learned from solution support, a testing environment and a CSfC Initial Solution that implemented secure voice and data capabilities using a set of Suite B algorithms, modes of operation, standards, and protocols.

2 PURPOSE AND USE

This CP provides high-level reference designs and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List, available on the CSfC web page (http://www.nsa.gov/ia/programs/csfc_program), for their MA solution and properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 11, customers must ensure that the components selected from the CSfC Components List will provide the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold requirements, or the corresponding Objective Requirements applicable to the selected capabilities, must be implemented, as described in Sections 10-12.16.5.

Customers who want to use this CP must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

This document, the CSfC Mobile Access CP Version 1.8, dated March 2016, has not been approved by the IAD Director and is being released for the purpose of soliciting public comments.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the MA CP maintenance team at Mobile_Access@nsa.gov. MA CP solutions shall also comply with Committee on National Security System (CNSS) policies and instructions. Any conflicts identified between this CP and NSS or local policy should be provided to the MA CP Maintenance team.



Mobile Access Capability Package



3 LEGAL DISCLAIMER

This CP is provided “as is.” Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this CP, even if advised of the possibility of such damage.

The user of this CP agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney’s fees, court costs, and expenses, arising in direct consequence of Recipient’s use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer’s product or service.

4 DESCRIPTION OF THE MOBILE ACCESS SOLUTION

This CP describes a general MA solution to protect classified information as it travels across either an untrusted network or a network consisting of multiple classification levels. The solution supports connecting end-user devices (EUDs) to a classified network via two layers of encryption terminated on the EUD provided that the EUD and the network operate at the same security level. The MA solution uses two nested, independent tunnels to protect the confidentiality and integrity of data (including Voice and Video) as it transits the untrusted network. The MA solution utilizes Internet Protocol Security (IPsec) as the outer tunnel and, depending on the solution design, IPsec or Transport Layer Security (TLS) as the inner layer of protection.

Throughout this CP, the term “Inner Encryption Component” is used to refer generically to the component (device or software application) that terminates the inner layer of encryption. An Inner Encryption Component can be a VPN Component or a TLS Component that is in the infrastructure or part of an EUD. The term “VPN Component” refers generically to both VPN Gateways and VPN Clients in situations where the differences between the two are unimportant. The term “TLS Component” is used to denote a component that implements TLS between the infrastructure (TLS-Protected Server or Secure Real-time Transport Protocol (SRTP) Endpoint) and EUDs (TLS Client or SRTP Client) in accordance with this CP (see Sections 5.6 and 5.8 respectively). There are two EUD solution designs: VPN EUD and TLS EUD. The term “EUD” is used to refer generically to both designs where the differences between them



Mobile Access Capability Package



are unimportant. Finally, the term “Dedicated Outer VPN” is used to describe a dedicated piece of hardware that can be part of an EUD and terminates the outer layer of IPsec encryption.

Table 1. Overview of Mobile Access CP Terminology

	VPN EUD	TLS EUD
Inner Encryption Component	IPsec provided by VPN Client	TLS or SRTP provided by TLS-Protected Server, SRTP Endpoint, TLS Client, OR SRTP Client
Outer Encryption Component	IPsec provided by VPN GW OR VPN Client	IPsec provided by VPN GW OR VPN Client

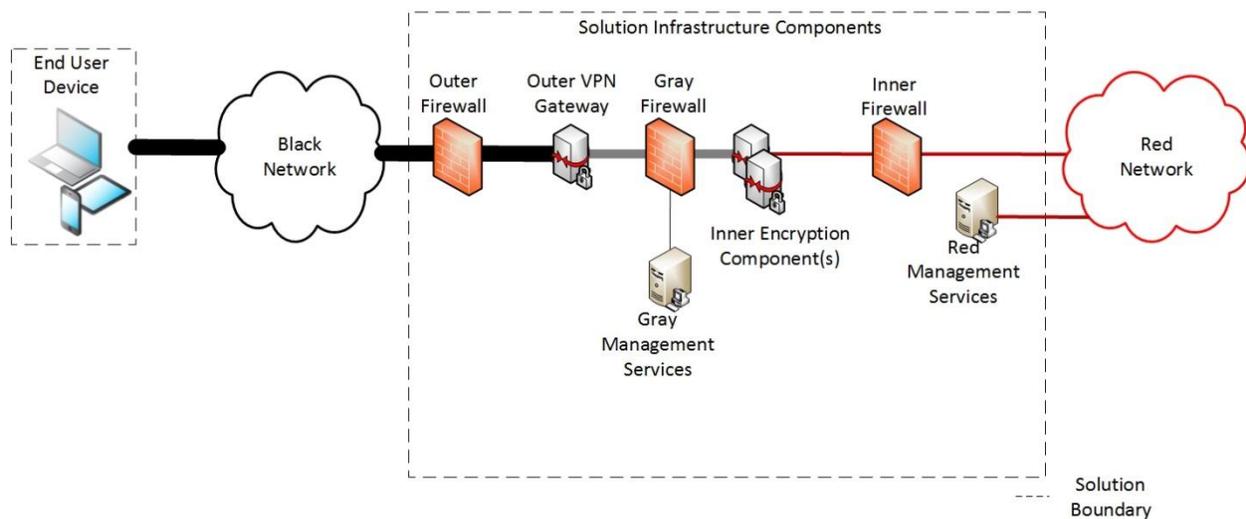


Figure 1. Overview of Mobile Access Solution

As shown in Figure 1, before being sent across the untrusted network, classified data is encrypted twice: first by an Inner Encryption Component, and then by an Outer VPN Component. At the other end of the data flow, the received packet is correspondingly decrypted twice: first by an Outer VPN Component, and then by an Inner Encryption Component.

All Encryption Components are within the CSfC Solution Boundary. The MA CP Version 1.8 no longer allows the use of existing Classified Enterprise Network Encryption Components to provide the inner layer of protection.

MA solution components are managed using Red Management Services for Inner Encryption Components and Gray Management Services for Outer Encryption Components. The Gray Management Services include an administration workstation, a Gray firewall, a Security Information and Event Monitoring (SIEM) Component, Intrusion Detection System (IDS)/Intrusion Protection System (IPS) and



Mobile Access Capability Package



any additional components located between the Outer VPN Gateway and Inner Encryption Components. Gray Management Services may also include a locally run outer Certificate Authority (CA), Certificate Revocation List (CRL) Distribution Point (CDP), and/or Authentication Server. The Red Management Services include an administration workstation, an inner firewall, and other components within the Red Network. The Red Management Services may also manage a locally run inner CA and, optionally, a locally-run outer CA. In addition, the MA CP allows customers to leverage an existing Enterprise Public Key Infrastructure (PKI) to issue certificates to Outer VPN Components and Inner Encryption Components. To utilize an existing Enterprise Root CA at least two separate subordinate CAs must be utilized: one to issue Certificates for Outer VPN Components and the other to issue certificates for Inner Encryption Components.

The EUDs utilized within the MA CP are form-factor agnostic. Typical MA CP EUDs include smart phones, tablets, and laptops. An MA CP EUD can be composed of multiple physical devices (for example a VPN Gateway and a computing device) all collectively referred to as the EUD. Although the CP allows flexibility in the selection of the EUD, the customer and Integrator must ensure that EUDs meet all applicable requirements for the planned solution design. Section 4.2.1 describes in detail the differences between the VPN EUD and TLS EUD solution design options.

The MA CP instantiations are built using products from the CSfC Components List (see Section 11). Customers who are concerned that their desired products are not yet on the CSfC Components List are encouraged to contact the appropriate vendors and encourage them to sign a Memorandum of Agreement (MoA) with NSA and start the National Information Assurance Partnership (NIAP) evaluation process which will enable them to be listed on the CSfC Components List. Products listed on the CSfC Components List are not guaranteed to be interoperable with all other products on the CSfC Components List. Customers and Integrators should perform interoperability testing to ensure the components selected for their MA Solution are interoperable. If you need assistance obtaining vendor POC information, please email csfc_components@nsa.gov.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a NIAP-evaluated component in a CSfC solution may invalidate its certification and trigger a revalidation process. To avoid delays, customers or Integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (see http://www.niap-ccves.org/Documents_and_Guidance/ccves/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification. In the case of a modification to a component, NSA's CSfC Program Management Office requires a statement from NIAP that the modification does not alter the certification or the security of the component. Modifications that trigger the revalidation process include, but are not limited to, modifying the original equipment manufacturers' code (to include digitally signing the code) or neglecting to leverage the baseline NIAP-evaluated configuration.



Mobile Access Capability Package



4.1 NETWORKS

This CP uses the following terminology to describe the various networks that comprise a MA solution and the types of traffic present on each: Red, Gray, and Black. The terms Red, Gray, and Black refer to the level of protection applied to the data as described below.

4.1.1 RED NETWORK

Red data consists of unencrypted classified data and a Red network contains only Red data. Red networks are under the control of the solution owner or a trusted third party.

The Red network begins at the internal interface(s) of Inner Encryption Components located between the Gray firewall and inner firewall. EUDs access the Red network through the two layers of nested encryption described in this CP. For example, an Inner VPN Gateway located between the Gray firewall and inner firewall terminates the inner layer of IPsec encryption from a VPN EUD. Once a successful IPsec connection is established, the EUD is given access to classified services such as web, email, Virtual Desktop Infrastructure (VDI), voice, etc.

In some instances, when the MA infrastructure is designed to support TLS EUDs, the TLS-Protected Server or SRTP Endpoint, which terminates the inner layer of encryption, will implement a TLS-Protected Server that includes both Gray and Red network interfaces located between the Gray firewall and inner firewall. This TLS-Protected Server terminates the TLS connection from the EUD and acts as a proxy to Red Services located outside of the CSfC Solution Boundary. A similar situation exists for SRTP when using a VoIP Gateway/Border Controller to terminate the SRTP traffic for an EUD and relaying the data to the Red network. When a VoIP Gateway/Border Controller terminates the inner layer of SRTP, desktop phones in the Red network are not included in the Solution Boundary.

Red networks may only communicate with an EUD through the MA solution if both operate at the same security level.

4.1.2 GRAY NETWORK

Gray data is classified data that has been encrypted once. Gray networks are composed of Gray Data. Gray networks are under the physical and logical control of the solution owner or a trusted third party.

The Gray network is physically treated as a classified network even though all classified data is singly encrypted. If a solution owner's classification authority determines that data on a Gray network is classified, perhaps by determining the Internet Protocol (IP) addresses are classified at some level, then the MA solution described in this CP cannot be implemented, as it is not designed to provide two layers of protection for any classified information on the Gray network.

Gray network components consist of the Outer VPN Gateway, Gray firewall, and Gray Management Services. All Gray network components are physically protected at the same level as the Red network



Mobile Access Capability Package



components of the MA infrastructure. Gray Management Services are physically connected to the Gray firewall and include, at a minimum, an administration workstation and SIEM. The MA CP requires the management of Gray network components through the Gray administration workstation. As a result, neither Red nor Black administration Workstations are permitted to manage the Outer VPN Gateway, Gray firewall, or Gray Management Services. Additionally, the Gray administration workstation is prohibited from managing Inner Encryption Components. These Inner Encryption Components must be managed from a Red administration workstation.

4.1.3 BLACK NETWORK

A Black network contains classified data that has been encrypted twice. The network connecting the Outer VPN Components together is a Black network. Black networks are not necessarily, and often will not be, under the control of the solution owner and may be operated by an untrusted third party.

The MA CP allows EUDs to operate over any Black network when used in conjunction with a Government-owned Retransmission Device (RD) or a physically separate Dedicated Outer VPN to establish the Outer IPsec Tunnel. An RD provides a connection to the MA solution infrastructure via any Black network and interfaces with the EUD using Wi-Fi or an Ethernet cable; however, the CP does not permit the use of Ethernet over USB. Black networks include non-domestic cellular carrier networks, public Wi-Fi networks, wired connections (to the Internet for example), and any other wireless or wired networks.

The Government-owned RD is a category of devices that includes Wi-Fi hotspots and mobile routers (WAP?). On the external side, the RD can be connected to any type of medium (e.g., cellular, Wi-Fi, SATCOM, Ethernet) to gain access to a Wide Area Network. On the internal side, the RD is connected to EUDs either through an Ethernet cable or Wi-Fi. When the RD is a Wi-Fi access point connected to the EUD (or multiple EUDs), the Wi-Fi network shall implement Wi-Fi Protected Access II (WPA2) with either Pre-Shared Key (PSK) or WPA2 Enterprise (see Section 9.3 for additional details regarding key and certificate management for WPA2). The EUD shall be configured to only permit connections to authorized RDs. RDs are only permitted to establish connectivity to the Black network, and may not be placed between an Outer Encryption Component and Inner Encryption Component.

The CP also allows connectivity without the use of an RD or dedicated Outer VPN if any of the following transport networks are utilized: domestic cellular providers, Government Private Cellular Networks, or Government Private Wireless Networks. Domestic cellular providers enable connectivity through cellular base stations geographically located within the United States of America. Government Private Cellular Networks are defined as cellular base stations that are owned and operated exclusively by the United States Government (such as in tactical environments). Finally, Government Private Wireless Networks denote Wi-Fi connectivity by a Wireless Local Area Network (WLAN) accredited by a Government Authorizing Official (AO). These Wi-Fi networks must comply with applicable organization policies. Within the Department of Defense (DOD) the applicable policy is DOD Instruction (DODI) 8420.01. At a



Mobile Access Capability Package



minimum, these Wi-Fi networks must implement WPA2 with PSK; however, WPA2 with certificate-based authentication is preferred. When Government Private Wireless Networks utilize certificate-based authentication, they cannot share the outer tunnel CA or inner tunnel CA certificate management services. WPA2 protects the Black transport network, but does not count as one of the layers of CSfC Data-in-Transit encryption.

Table 2. Acceptable Black Transport Networks

	VPN EUD	TLS EUD
Any Black Transport Network	Government RD OR VPN Gateway	Government RD OR VPN Gateway
Domestic Cellular, Government Private Cellular, or Government Private Wireless	No additional requirements	No additional requirements



Mobile Access Capability Package

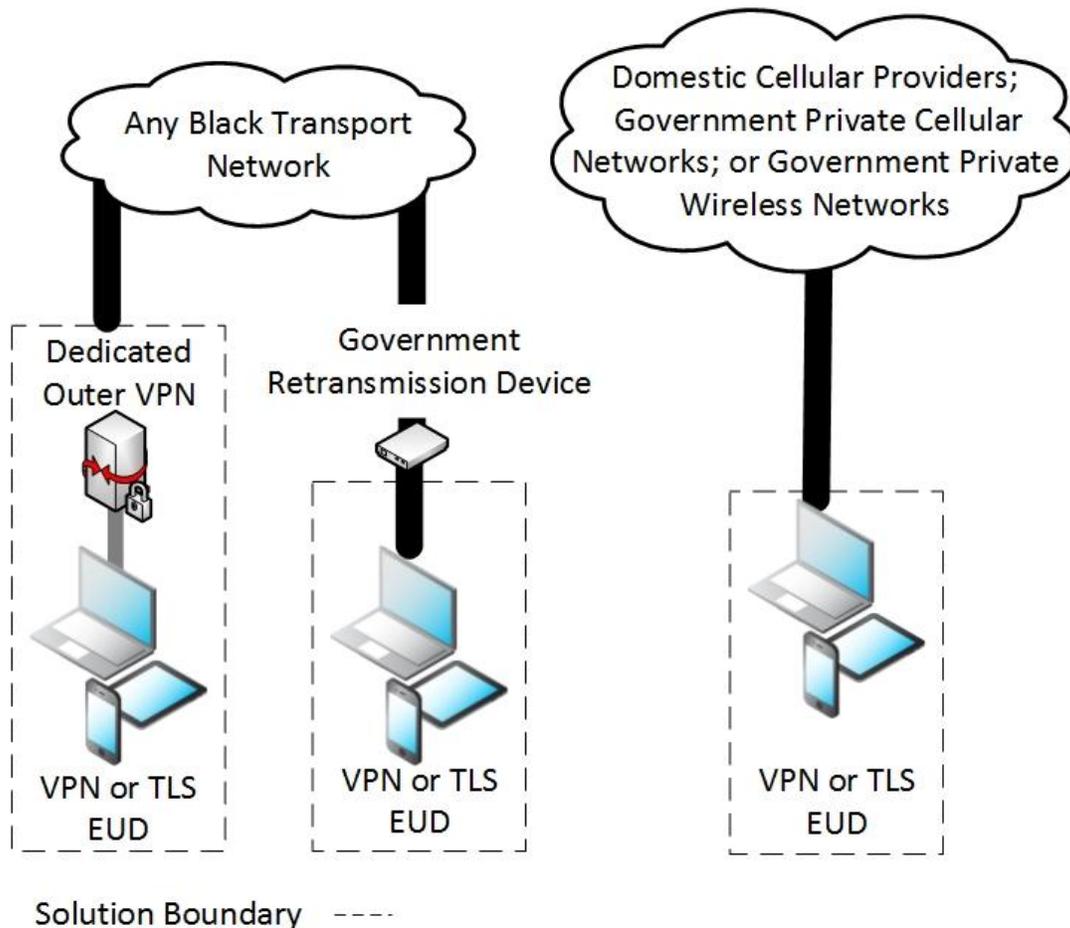


Figure 2. Acceptable Black Transport Networks

As shown in Figure 2, both EUD designs can connect to the MA solution over domestic cellular, Government Private Cellular, or Government Private Wireless Networks without the need for a separate, standalone piece of hardware. When connecting over any other black transport network, EUDs must use a Dedicated Outer VPN or a Government RD to connect to the MA solution. When an EUD includes a Dedicated Outer VPN, that VPN is utilized to establish the outer layer of IPsec to the government infrastructure and is included within the CSfC Solution Boundary. The Dedicated Outer VPN must be connected to the computing platform utilizing an Ethernet cable or WPA2 (see Section 12.9 and Section 12.10). The computing platform then terminates the inner layer of encryption. Although only required as described above, a Dedicated Outer VPN can be utilized to connect to any transport network for any of the EUD solution designs. Similarly, an EUD can utilize a Government RD to connect to any transport network. The Government RD is outside the CSfC Solution Boundary, but acts as an intermediary between the desired transport network and the EUD.



Mobile Access Capability Package



4.1.4 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or not, that is being passed through the MA solution. The MA solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Black network is encapsulated within the Encapsulating Security Payload (ESP) protocol. All data plane traffic within the Gray network is encapsulated within ESP, TLS, or SRTP. When utilizing a dedicated outer VPN with wireless connectivity, Gray data plane traffic between the computing platform and dedicated VPN is encapsulated within ESP and WPA2.

Management plane traffic is used to configure and monitor solution components. It includes the communications between a system administrator and a component, as well as the logs and other status information forwarded from a solution component to a SIEM or similar repository. Management plane traffic on Red and Gray networks is (must be?) encapsulated within the Secure Shell (SSH), ESP, or TLS protocol.

Control plane traffic consists of standard protocols necessary for the network to function. Unlike data or management plane traffic, control plane traffic is typically not initiated directly on behalf of a user or a system administrator. Examples of control plane traffic include, but are not limited to, the following:

- Network address configuration (e.g. Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery Protocol (NDP), etc.)
- Address resolution (e.g. Address Resolution Protocol (ARP), NDP, etc.)
- Name resolution (e.g. Domain Name System (DNS), etc.)
- Time synchronization (e.g. Network Time Protocol (NTP), Precision Time Protocol (PTP), etc.)
- Route advertisement (e.g. Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Border Gateway Protocol (BGP), etc.)
- Certificate status distribution (e.g. Online Certificate Status Protocol (OCSP), HTTP download of CRLs, etc.)

The MA CP explicitly prohibits the use of most control plane traffic for EUDs that utilize a single computing device to provide both the inner and outer layer of encryption (see Appendix D. End User Device Implementation Notes). The MA CP does not allow route advertisement or certificate status distribution to ingress/egress from the Black transport network for these EUDs. As a result, the implementing organization must implement procedures to handle a situation in which the certificate of an Outer VPN Gateway is revoked. EUDs are configured for all IP traffic to flow through the Outer IPsec VPN Client with the exception of control plane protocols necessary to establish the IPsec tunnel. The control plane necessary to establish the IPsec tunnel is limited to Internet Key Exchange (IKE), address



Mobile Access Capability Package



configuration, time synchronization, and in some cases name resolution traffic. EUDs selected from the CSfC Components List should utilize NIAP evaluated configurations to ensure that IP traffic flows through the Outer IPsec VPN Client. Upon establishing the outer VPN tunnel, the CP does not impose detailed requirements restricting control plane traffic in the Gray and Red networks.

Restrictions are also placed on control plane traffic for the Outer VPN Gateway. The Outer VPN Gateway is prohibited from implementing routing protocols on external and internal interfaces. The Outer VPN Gateway can (must) rely on the Outer firewall to perform routing functionality.

Except as otherwise specified in this CP, the usage of specific control plane protocols is left to the solution owner to approve. The solution owner must disable or block any unapproved control plane protocols.

Data plane and management plane traffic are generally required to be separated from one another by using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray data network and a Gray management network that are separate from one another, where the components on the Gray management network are used to manage the components on the Gray data network. The Gray management network is separated from the Gray data network via the Gray firewall. The Gray firewall utilizes an Access Control List (ACL) to ensure that only appropriate Gray Management Services (i.e. administration workstation, SIEM or Network Time Server) can communicate with the Outer VPN Gateway and EUDs that have established an outer VPN tunnel. The Gray firewall is also responsible for ensuring that Gray Management Services are only capable of flowing in the appropriate direction. For example, SSH traffic is permitted to initiate from an administration workstation to the Outer VPN Gateway, but not from the Outer VPN Gateway to any Gray Management Services. Conversely, system log data is permitted from the Outer VPN Gateway to the Gray SIEM, but is not permitted from Gray Management Services to the Outer VPN Gateway. Given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated, unless otherwise specified.

4.2 HIGH-LEVEL DESIGN

The MA solution is adaptable to support multiple capabilities, depending on the needs of the customer implementing the solution. The supported EUD capabilities are mutually exclusive; if a customer chooses to implement an EUD using two layers of IPsec, then the Inner TLS Client would not be included as part of that EUD implementation. Similarly, if a customer only needs a secure voice capability, then the Inner IPsec Component would not be included as part of that EUD implementation. Although the EUD solution designs are mutually exclusive, the infrastructure may be configured to support both EUD solution designs (see 0). This enables implementation of both types of EUDs based on use cases and device features. Any implementation of the MA solution must satisfy all of the applicable requirements specified in this CP, as explained in Sections 11 and 12.



Mobile Access Capability Package



4.2.1 END USER DEVICES

This CP uses the concept of an EUD, which is either a computing device, such as a smart phone, laptop, or tablet, or a Dedicated Outer VPN. The EUD provides two layers of protection for data in transit to tunnel through the Black network and access classified data on the Red network. In some instances, an EUD encompasses more than one piece of hardware (e.g. computing device and Dedicated Outer VPN) each of which perform a layer of encryption. Where more than one piece of hardware is used, each component is included as part of the EUD and are within the CSfC Solution Boundary. EUDs are dedicated to a single classification level and can only be utilized to access a Red network of the same classification. There are two EUD designs which can be implemented as part of a MA solution. Each of the EUD designs share many requirements in common, but also have unique requirements specific to that design:

- 1) **IPsec-IPsec (VPN EUD):** Utilizes two IPsec tunnels to connect to the Enterprise/Red network. Such an EUD includes both an Inner VPN Client and Outer VPN Component to provide the two layers of IPsec. Throughout the document this EUD design is referred to as the “VPN EUD”. VPN EUDs can be implemented utilizing combinations of IPsec VPN Clients and IPsec Gateways (see Appendix D. End User Device Implementation Notes). For example, a VPN EUD can be implemented on a computing device with two VPN Clients running on separate IP stacks. Similarly, the MA CP allows a VPN EUD to utilize a Dedicated Outer VPN to provide the outer layer of IPsec encryption and a VPN Client installed on a computing device to provide the inner layer of encryption.
- 2) **IPsec-TLS (TLS EUD):** Utilizes an outer layer of IPsec encryption and an inner layer of TLS encryption to access the Red network. Throughout the document this EUD design is referred to as the “TLS EUD”. The outer layer of encryption can be provided by either an IPsec VPN Client or a standalone IPsec VPN Gateway. The inner layer of encryption is then provided by a TLS Client. The EUD TLS Client includes a number of different options which can be selected, in accordance with the CP requirements, to meet the operational needs of the customer. The EUD TLS Clients include, but are not limited to, web browsers, email clients, and VoIP applications. Traffic between the TLS EUD Client and the TLS-Protected Server is encrypted with TLS or in some instances SRTP. When SRTP is utilized, session keys are first exchanged using Session Initiation Protocol (SIP) over TLS.



Mobile Access Capability Package

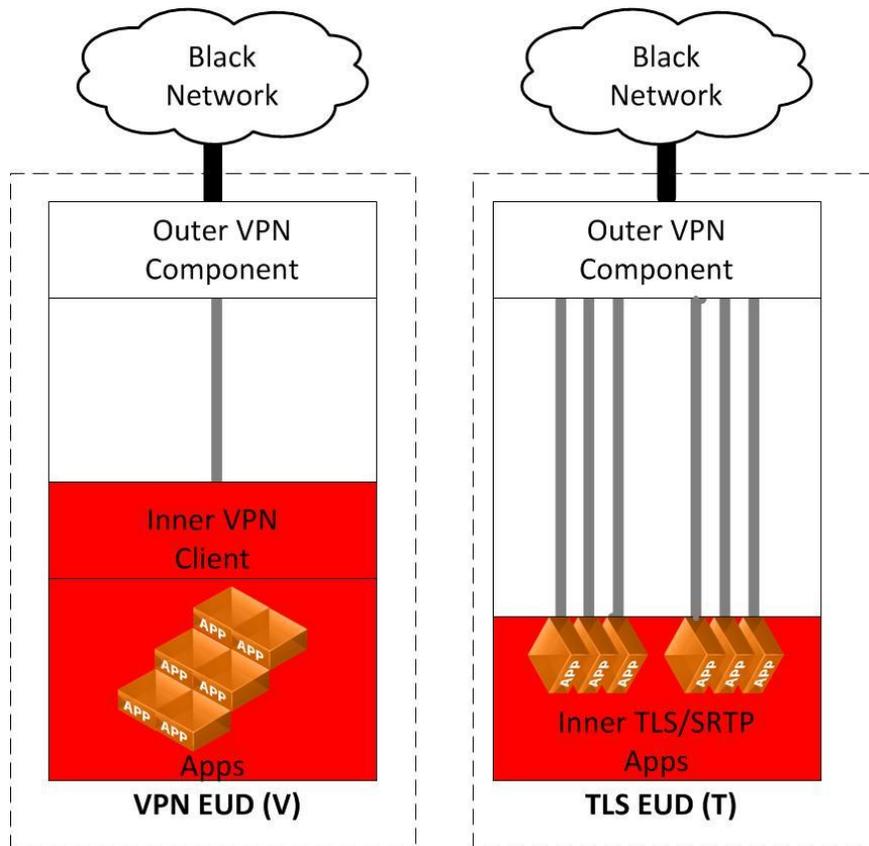


Figure 3. EUD Solution Designs

Figure 3 depicts the two EUD solution designs available as part of the MA CP. In each design the Outer VPN Component is utilized to establish an IPsec tunnel to the Outer VPN Gateway of the MA solution infrastructure. In either EUD design, this Outer VPN Component must be selected from the CSfC Components list and could be either a VPN Client or a VPN Gateway. If a dedicated outer VPN is utilized to provide the outer IPsec tunnel, then the computing platform must be connected to the dedicated outer VPN Gateway utilizing an Ethernet cable or WPA2.

The inner layer of encryption for VPN EUDs is provided by a VPN Client. The inner VPN Client must be selected from the CSfC Components List (see Section 11). If VPN Clients are used for both the inner and outer layers of encryption then they must utilize a different IP stack, and are generally implemented using virtualization.

The inner layer of encryption for TLS EUDs is provided by either TLS or SRTP. Every application that performs TLS or SRTP must be selected from the CSfC Components List.

The Mobile Access CP allows two different deployment options pertaining to the use and handling of an EUD while powered off:



Mobile Access Capability Package



1. **EUD with DAR:** To implement Data-at-Rest (DAR) on an EUD, the DAR solution shall be approved by NSA – either as a tailored solution, or compliant and registered with NSA’s DAR CP for the protection of information classified at the level of the Red network connected to the EUD. Specification of such a DAR solution is outside the scope of this CP, but can be found in the DAR CP. Positive control of the EUD must be maintained at all times.
2. **Classified EUD:** The EUD can only be used when applying physical security measures approved by the AO. EUDs are not subject to special physical handling restrictions beyond those applicable for classified devices as they can rely on the environment they are utilized within for physical protection. If this design option is selected, then the EUDs must be treated as classified devices at all times. The EUD in this case must enable the native platform DAR protection in order to protect the private keys stored on it from disclosure and increase the difficulty of tampering with the software and configuration. Positive control of the EUD must be maintained at all times.

While powered on, an EUD is classified at the same level of the connected Red network, since classified data may be present in volatile memory and/or displayed on screen. To mitigate the risk of accidental disclosure of classified information to unauthorized personnel while the EUD is in use, the customer must define and implement an EUD user agreement that specifies the rules of use for the system. The customer must require that all users accept the user agreement and receive training on how to use and protect their EUD before being granted access. There is no limit to the number of EUDs that may be included in an MA solution.

4.2.2 INDEPENDENT SITE

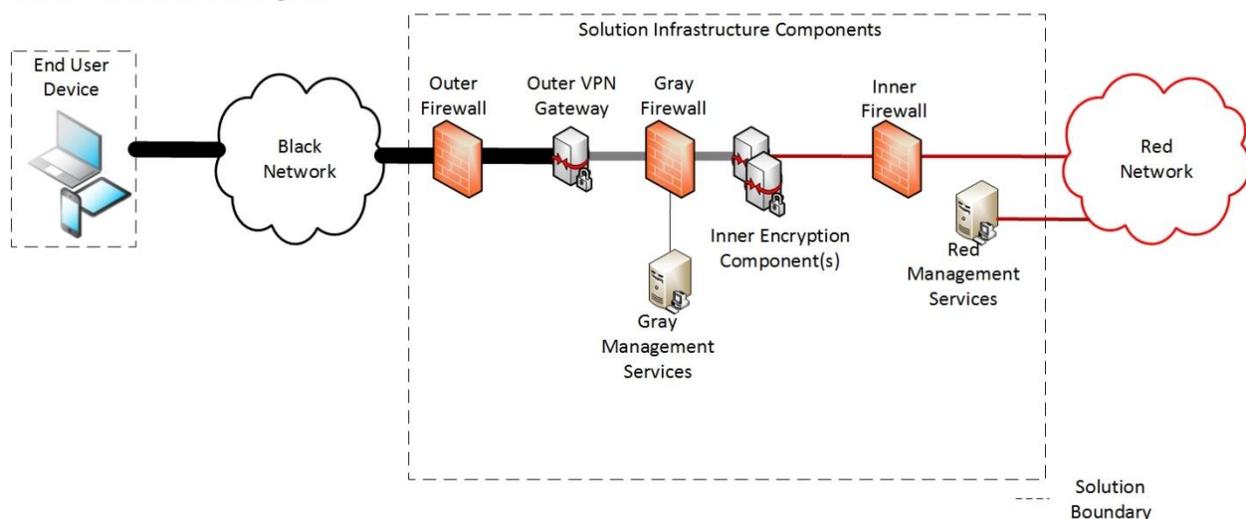


Figure 4. EUDs Connected to Independent Site



Mobile Access Capability Package



Figure 4 depicts a single Red network connected to EUDs that operate at the same security level through the MA solution. Here, the Red network has at least two Encryption Components associated with it: one or more Inner Encryption Components connected to the Red network, and an Outer VPN Gateway between the Inner Encryption Components and the Black network. There are two layers of encryption between any EUD communicating with the Red network: one IPsec tunnel between their Outer VPN Components, and a second IPsec, TLS or SRTP tunnel depending on the selected EUD design(s).

For independent sites, administration is performed at that site for all components within the Solution Boundary, including the Outer VPN Gateway, Gray Management Services, Inner Encryption Components, Red Management Services, firewalls, and EUDs. Independent sites are not interconnected with other infrastructure sites through the MA solution; therefore, management, data plane, and control plane traffic between solution infrastructure sites are outside the scope of the MA CP. If two or more sites must be interconnected, customers may also register the MA solution against the VPN CP or utilize an NSA-Certified encryptor.



Mobile Access Capability Package



Note that while Figure 4 depicts only a single EUD, this solution does not limit the number of EUDs being implemented.

4.2.3 MULTIPLE SITES

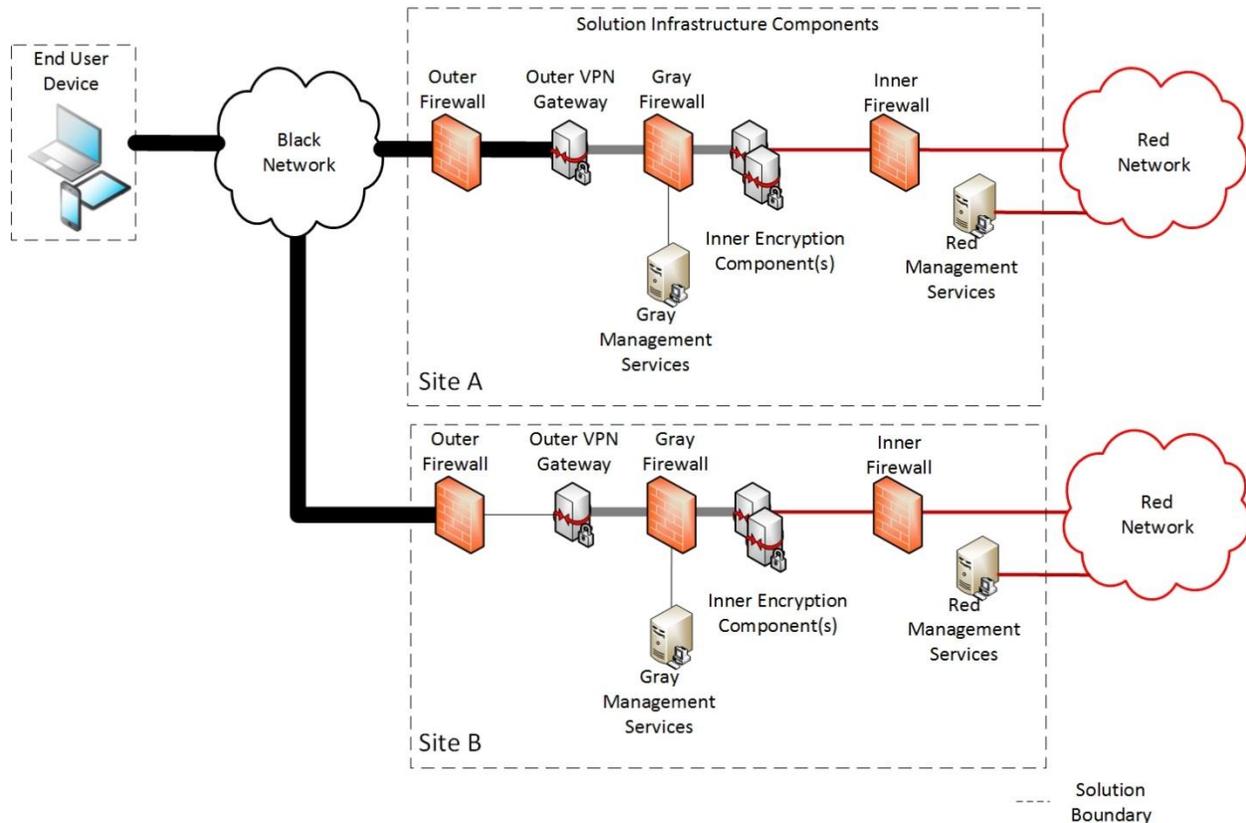


Figure 5. Multiple Mobile Access Solution Infrastructures supporting EUDs

Figure 5 depicts two MA solution infrastructures that an EUD can connect to in order to access different Red network services. Customers may want to implement multiple solution infrastructures to support Continuity of Operations or provide better performance based on geographic location of EUDs or Red services. The multiple solution infrastructures may be interconnected using an NSA-approved solution such as the Virtual Private Network (VPN) CP or a NSA-Certified encryptor; however, connectivity of Solution Infrastructure Components is outside the scope of the MA CP.

Note that while Figure 5 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in Figure 5.



Mobile Access Capability Package

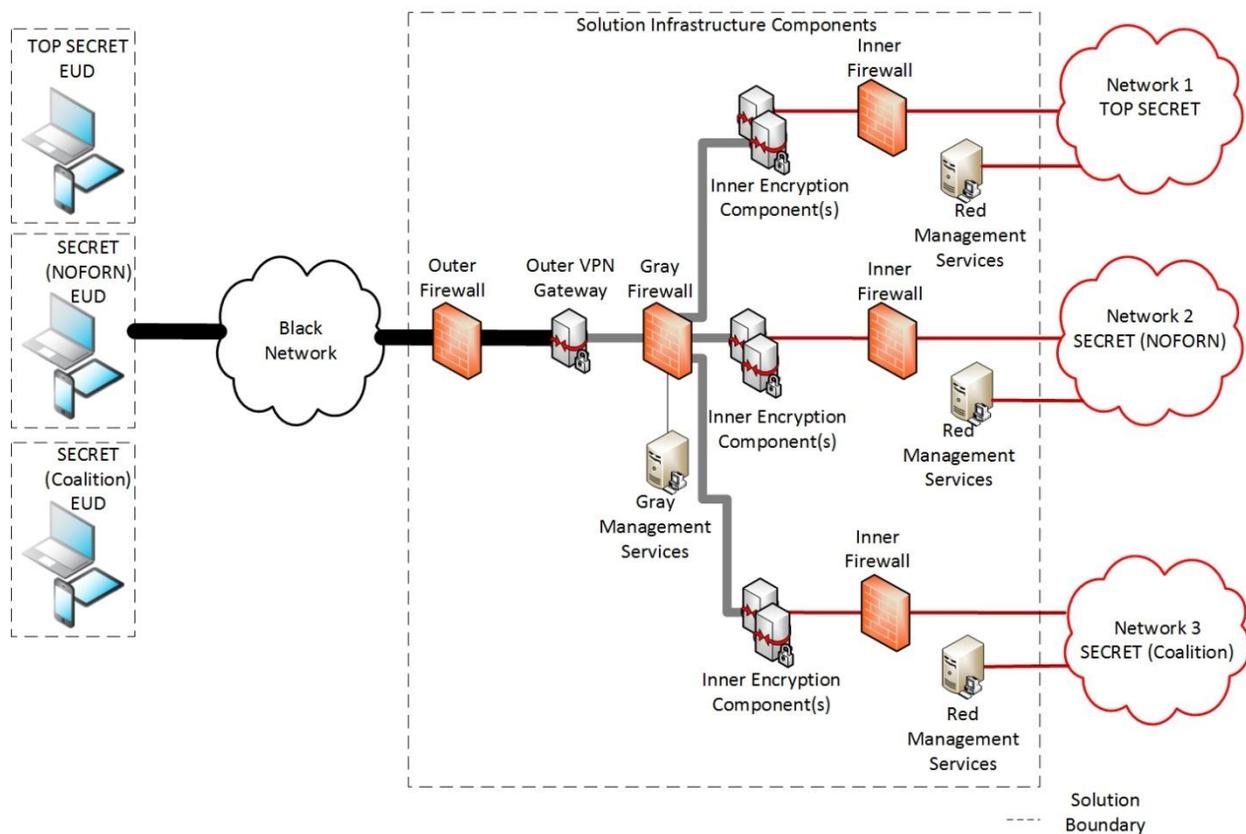


Figure 6. Mobile Access Solution Supporting Multiple Security Levels

4.2.4 MULTIPLE SECURITY LEVELS

A single implementation of the MA solution may support multiple Red networks of different security levels. The MA solution provides secure connectivity between EUDs and the Red network of the same security level while preventing EUDs from accessing Red networks of different security levels. This enables a customer to use the same physical infrastructure to carry traffic from multiple networks. Although each Red network will still require its own Inner Encryption Component(s), a site may use a single Outer VPN Gateway to encrypt and transport traffic that has been encrypted by Inner Encryption Components of varying security levels.

There is no limit to the number of different security levels that an MA solution may support.

MA solutions supporting multiple security levels may include independently managed sites (see Section 4.2.2) or multiple sites (see Section 4.2.3). In all cases, separate CAs and management devices are needed to manage the Inner Encryption Components and Inner Firewall at each security level. For example, Figure 6 depicts an independent site with multiple security levels. Network 1 and Network 2 each have their own CA and management devices which prevent EUDs from being able to authenticate with the incorrect network.



Mobile Access Capability Package



In addition to separate Inner Encryption Components and CAs, an Authentication Server must be utilized to allow the use of an Outer VPN Gateway for multiple security levels. The Authentication Server resides within the Gray Management Network and validates that certificates are signed by the correct CA, are still within their validity period, and have not been revoked. The Authentication Server also parses the certificate for an Organizational Unit (OU) field or policy Object Identifiers (OIDs) that are assigned to a specific inner network. After successful authentication, the Authentication Server provides a RADIUS accept message to the Outer VPN Gateway along with a Vendor-Specific Attribute (VSA). The Outer VPN Gateway utilizes the VSA to assign the proper network and firewall rules such that an EUD can only reach the appropriate Inner Encryption Components.

4.3 RATIONALE FOR LAYERED ENCRYPTION

A single layer of Suite B encryption, properly implemented, is sufficient to protect classified data in transit across an untrusted network. The MA solution uses two layers of Suite B encryption not because of a deficiency in the cryptographic algorithms themselves, but rather to mitigate the risk that a failure in one of the components, whether by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability, results in exposure of classified information. The use of multiple layers of protection reduces the likelihood of any one vulnerability being used to exploit the full solution, particularly if the layers exhibit suitable independence.

If an Outer VPN Component is compromised or fails in some way, the Inner Encryption Component can still provide sufficient encryption to prevent the immediate exposure of classified data to a Black network. In addition, the Gray firewall can indicate that a failure of the Outer VPN Gateway has occurred, since the filtering rules applied to its external network interface will drop and log the receipt of any packets not associated with an Inner Encryption Component. Such log messages indicate that the Outer VPN Gateway has been breached or misconfigured to permit prohibited traffic to pass through to the Inner encryption component.

Conversely, if the Inner Encryption Component is compromised or fails in some way, the Outer VPN Gateway can likewise provide sufficient encryption to prevent the immediate exposure of classified data to a Black network. As in the previous case, the Gray firewall filtering rules applied to its internal network interfaces will drop and log the receipt of any packets not associated with an Inner Encryption Component. Such log messages indicate that the Inner Gateway has been breached or misconfigured to permit prohibited traffic to pass through to the Outer VPN Gateway.

If both the Outer and Inner Gateways are compromised or fail simultaneously, then it may be possible for classified data from the Red network to be sent to a Black network without an adequate level of encryption. The security of the MA solution depends on preventing this failure mode by promptly remediating any compromises or failures in one Encryption Component before the other also fails or is compromised.



Mobile Access Capability Package



Diversity of implementation is needed between the components in each layer of the solution in order to reduce the likelihood that both layers share a common vulnerability. The CSfC Program recognizes two ways to achieve this diversity. The first is to implement each layer using components produced by different manufacturers. The second is to use components from the same manufacturer, where that manufacturer has provided NSA with sufficient evidence that the implementations of the two components are independent of one another. The CSfC web page (http://www.nsa.gov/ia/programs/csfc_program) contains details for how a manufacturer can submit this evidence to NSA and what documentation must be provided. Customers that wish to use products from the same manufacturer in both layers must contact their NSA/IAD Client Advocate to confirm that NSA has accepted the manufacturer's claims before implementing their solution.

4.4 AUTHENTICATION

The MA solution provides mutual device authentication between Outer VPN components and between Inner Encryption components via public key certificates. This CP requires all authentication certificates issued to Outer VPN components and Inner Encryption components be Non-Person Entity (NPE) certificates, except in the case when TLS EUDs are implemented. In addition, NPE certificates issued to Outer VPN Gateways may need to assert the IP address of the Outer VPN Gateway in either the Common Name field of the certificate Distinguished Name, or in the Subject Alternative Name certificate extension. The EUD may be required to check the IP address asserted in the Outer VPN Gateway certificate and ensure it is the same IP address registered in the EUD.

Following the two layers of device authentication, VPN EUDs require the user to authenticate to the network before gaining access to any classified data (e.g., username/password, user certificate). TLS EUDs may utilize a device certificate or a user certificate. When a device certificate is used, the user must also authenticate to the Red network before gaining access to any classified data in the same manner as a VPN EUD (e.g., username/password, user certificate). When a user certificate is used, the user certificate authenticates the inner layer of TLS encryption and authenticates the user for access to the requested classified data. In this latter case, it is recommended that additional access controls, such as whitelists, be implemented in conjunction with the user certificate to control access to Red network services.

In addition to authentication for the outer and inner layer of encryption, the MA CP requires user-to-device authentication. This authentication occurs between the user and the computing device (which processes Red data) of an EUD. In some instances the computing device may be physically separate from the component of the EUD which provides the outer layer of encryption (for example, a Dedicated Outer VPN Gateway provides the outer layer of encryption). The MA CP requires EUD components utilize a minimum of a four-character, case-sensitive, alpha-numeric password to authenticate to the device. This password can be used both for decrypting the platform encryption as well as for unlocking the screen. EUD components, which are selected from the Mobile Platform section of the CSfC Components,



Mobile Access Capability Package



are able to utilize a relatively short authentication factor since they are backed by a hardware root of trust which is evaluated during the NIAP certification.

4.5 OTHER PROTOCOLS

Throughout this document, when IP traffic is discussed, it can refer to either IPv4 or IPv6 traffic, unless otherwise specified, as the MA solution is agnostic to most named data handling protocols.

Public standards conformant Layer 2 control protocols are allowed as necessary to ensure the operational usability of the network. This CP is agnostic with respect to Layer 2; specifically, it does not require Ethernet. Public standards conformant Layer 3 control protocols may be allowed based on local AO policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray network multicast messages and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) may also be allowed depending on local AO policy. Multicast messages received on external interfaces of the Outer VPN component shall be dropped.

It is expected that the MA solution can be implemented in such a way as to take advantage of standards-based routing protocols that are already being used in the network. For example, networks that currently use Generic Routing Encapsulation (GRE) or OSPF protocols can continue to use these in conjunction with this solution to provide routing as long as the AO approves their use.

4.6 AVAILABILITY

The high-level designs described in Section 4.2 are not designed with the intent of automatically providing high availability. Supporting solution implementations for which high availability is important is not a goal of this version of the CP. However, this CP does not prohibit adding redundant components in parallel to allow for component failover or to increase the throughput of the MA solution, as long as each redundant component adheres to the requirements of this CP. The CP does not limit the number of Outer VPN Gateways or Inner Encryption components that can be implemented for high availability in a MA Solution.

5 INFRASTRUCTURE COMPONENTS

In the high-level designs discussed in the previous section, all communications flowing across a Black network are protected by at least two layers of encryption, implemented using an outer IPsec VPN tunnel and an inner layer of IPsec, TLS, or SRTP encryption. Mandatory aspects of the solution infrastructure also include administration workstations, IDS/IPS, SIEM, firewalls, and CAs for key management using PKI.

Each infrastructure component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed necessary for the



Mobile Access Capability Package



solution. Components are selected from the CSfC Component List in accordance with the Product Selection requirements of this CP (see Section 11).

This section also provides details on additional components that can be added to the solution to help reduce the overall risk. However, where indicated in the text, these are not considered mandatory components for the security of the solution; therefore, this CP does not place configuration requirements on those optional components.

5.1 OUTER FIREWALL

The outer firewall is located at the edge of the Mobile Access solution infrastructure and is connected to the Black transport network.

The external interface of the outer firewall only permits IPsec IKE and ESP traffic with a destination address of the Outer VPN Gateway. Additionally, the external interface of the outer firewall can permit control plane traffic as necessary for connectivity and mission support. If the solution supports multiple security levels, the outer firewall will also permit Extensible Authentication Protocol (EAP) TLS traffic initiated by EUDs and destined for the Outer VPN Gateway.

The internal interface of the outer firewall only permits IPsec traffic with a source address of the Outer VPN Gateway and any necessary control plane traffic. The minimum requirements for port filtering on the outer firewall can be found in Section 12.11.

The outer firewall, selected from the CSfC Components List, must be physically separate from the Outer VPN Gateway, as depicted in Figure 4.

5.2 OUTER VPN GATEWAY

Authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules are all aspects fundamental to the security provided by VPN Gateways.

The external interface of the Outer VPN Gateway is connected to the internal interface of the outer firewall. The VPN Gateway establishes an IPsec tunnel with peer Outer VPN Components, which provides device authentication, confidentiality, and integrity of information traversing Black networks. VPNs offer a decreased risk of exposure of information in transit since any information that traverses a Black network is placed in a secure tunnel that provides an authenticated and encrypted path between the site and an EUD. The Outer VPN Gateway is implemented identically for all the high-level designs supporting a single security level, including when implemented as the Outer VPN Component for EUDs (see Section 6.1.2). When supporting Multiple Security Levels, the Outer VPN Gateway must utilize a gray Authentication Server and allow EAP-TLS on the external interface.



Mobile Access Capability Package



Similar to the outer firewall, the external interface of the Outer VPN Gateway only permits IPsec traffic and AO-approved control plane traffic. The internal interface of the Outer VPN Gateway is configured to only permit traffic with an IP address and port associated with Inner Encryption Components, Gray Management Services (i.e. SIEM and administration workstation), or Control Plane Component (i.e. DNS and NTP Servers in the Gray).

The Outer VPN Gateway is prohibited from implementing routing protocols on external and internal interfaces and must rely upon the outer firewall and/or Gray firewall to provide routing functionality. The Outer VPN Gateway, selected from the CSfC Components List, must be physically separate from the outer firewall and Gray firewall as depicted in Figure 4.

The Outer VPN Gateway is implemented in conjunction with a Gray Authentication Server when multiple security levels are implemented (as described in Section 4.2.4). The Outer VPN Gateway acts as an EAP pass-through for authentication between the EUD and Authentication Server. Upon successful mutual authentication, the Outer VPN Gateway receives a Remote Authentication Dial-In User Service (RADIUS) accept message and VSA for that specific EUD. The Outer VPN Gateway utilizes that attribute to assign the correct IP address and ACL to ensure that the EUD is only capable of reaching the correct Inner Encryption Component.

The Outer VPN Gateway cannot route packets between Gray and Black networks; any packets received on a Gray network interface and transmitted to a Black network interface must be transmitted within an IPsec VPN tunnel configured according to this CP.

5.3 GRAY FIREWALL

The Gray firewall is located between the outer VPN and inner encryption components. In addition to filtering EUD traffic, the Gray firewall also provides packet filtering for the Gray Management Services.

The external interface of the Gray firewall should only accept packets with a source address of the Outer VPN Gateway's DHCP pool for EUDs. The internal interface of the Gray firewall should only accept packets with a source address of the TLS-Protected server or the Inner VPN Gateway as part of an established communication session. When supporting multiple security levels the Gray Firewall also ensure that only EUDs and Inner Encryption components of the same security level are able to communicate.

In addition to EUD data traffic, the Gray firewall adjudicates traffic related to both the management of the Gray boundary and EUD control plane traffic. The Gray firewall, selected from the CSfC Components List, and must be physically separate from the Outer VPN Gateway and Inner Encryption Components, as depicted in Figure 4.



Mobile Access Capability Package



5.4 INNER FIREWALL

The inner firewall is located between the inner encryption components and the Red network. The external interface of the inner firewall should only accept inbound traffic with a source address of the TLS-Protected server or Inner VPN Component. The internal interface of the inner firewall should only allow outbound traffic from the Red enclave to the Inner VPN Component or the TLS-Protected server. The TLS-Protected servers include, but are not limited to: VoIP call managers, mobile device management (MDM) services, Virtual Desktop Infrastructure (VDI), and web server content.

The inner firewall, selected from the CSfC Components List, must be physically separate from the Inner Encryption Components.

5.5 GRAY MANAGEMENT SERVICES

Secure administration of components in the Gray network and continuous monitoring of the Gray network are essential roles provided by the Gray Management Services. The Gray Management Services are composed of multiple components that provide distinct security to the solution. The MA CP allows flexibility in the placement of some Gray Management Services, as described below. All components within the Gray Management Services are either directly or indirectly connected to the Gray firewall (e.g. multiple Gray Management Services connected to a switch which is connected to the Gray firewall). The Gray Management Services are physically protected as classified devices.

5.5.1 GRAY ADMINISTRATION WORKSTATION

The Gray administration workstations are responsible for maintaining, monitoring, and controlling all security functionality for the Outer VPN Gateway, Gray firewall, and all Gray Management Service components. The Gray administrative workstations are not permitted to maintain, monitor, or control Inner Encryption Components or Red Management Services. All Mobile Access solutions will have at least one Gray administrative workstation. Section 7 provides more detail on management of Mobile Access solution components.

5.5.2 GRAY SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

The Gray SIEM collects and analyzes log data from the Outer VPN Gateway, Gray firewall, and other Gray Management Service components. Log data may be encrypted between the originating component and the Gray SIEM with SSHv2, TLS, or IPsec to maintain confidentiality and integrity of the log data. At a minimum, an auditor reviews the Gray SIEM on a weekly basis. The SIEM is configured to provide alerts for specific events including if the Outer VPN Gateway or Gray firewall receive and drop any unexpected traffic which could indicate a compromise of the outer firewall or Outer VPN Gateway respectively. These functions can also be performed on a Red SIEM if a Cross Domain Solution (CDS) is utilized as described in this CP (see Section 8.5).



Mobile Access Capability Package



5.5.3 GRAY AUTHENTICATION SERVER

The Gray Authentication Server is only required for solutions supporting multiple security levels. The Authentication Server is responsible for performing mutual authentication with EUDs utilizing the Outer VPN Gateway as an EAP pass-through. In addition to verifying that certificates are signed by the correct CA, are within their validity period, and are not revoked, the Authentication Server parses the certificate for an OU or Policy OID. The OU or Policy OID is associated with the Red network which the EUD is permitted to establish an Inner IPsec connection or TLS session. Upon successful authentication of the EUD, the Authentication Server sends a Radius Access-Accept packet to the Outer VPN Gateway. The RADIUS Access-Accept packet includes an attribute derived from the OU or policy OID which the Outer VPN Gateway utilizes to apply ACLs and route the EUDs traffic to the proper Inner Encryption Component.

5.6 INNER ENCRYPTION COMPONENTS

The MA CP allows for the use of up to three different types of Inner Encryption Components: Inner VPN Gateway, Inner TLS-Protected Server, or Inner SRTP Endpoint. Inner VPN Gateways are always located between the Gray firewall and inner firewall. An Inner VPN Gateway will always have at least two interfaces, one external interface connected to the Gray firewall and one internal interface connected to the inner firewall.

Inner TLS-Protected Servers and Inner SRTP Endpoints are permitted to use a single interface or multiple interfaces. Similar to the Inner VPN Gateway, Inner TLS-Protected Servers and SRTP Endpoints with multiple interfaces can have one external interface connect to the Gray firewall and one internal interface connected to the inner firewall. If implemented with a single interface, then that interface establishes the inner layer of encryption and provides the classified data to the TLS EUD. An example of a TLS-Protected Server with a single interface is a web server located between the gray firewall and inner firewall that terminates the inner layer of encryption with HTTPS and directly returns the content to the TLS EUD. The TLS-Protected Servers and SRTP Endpoints must be placed between the Gray firewall and inner firewall but is not required to connect to the Red network or inner firewall if it is acting as the server for the EUDs.

An MA solution infrastructure may support both TLS EUDs and VPN EUDs. When supporting both TLS EUDs and VPN EUDs the solution infrastructure will always include an Inner VPN Gateway between the Gray firewall and inner firewall. This Inner VPN Gateway will terminate the inner layer of IPsec traffic for all VPN EUDs. Additionally, the solution infrastructure will include one or more TLS-Protected Servers. The TLS-Protected Servers are placed between the Gray firewall and inner firewall. The TLS-Protected Server(s) must be placed in parallel with the Inner VPN Gateway such that the TLS-Protected Server is not dependent on the Inner VPN Gateway to reach the Gray firewall or inner firewall (see Appendix D. End User Device Implementation Notes).



Mobile Access Capability Package



For load balance or other performance reasons, multiple Inner Encryption Components that comply with the requirements of the CP are acceptable.

5.6.1 INNER VPN GATEWAY

Similar to the Outer VPN Gateway, the Inner VPN Gateway provides authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules. The Inner VPN Gateway is located between the Gray firewall and the inner firewall. The Inner VPN Gateway is required to be implemented if supporting VPN EUDs.

The external interface of the Inner VPN Gateway is connected to the internal interface of the Gray firewall. The VPN Gateway establishes an IPsec tunnel with peer Inner VPN Components. Similar to the Outer VPN Gateway, the external interface of the Inner VPN Gateway only permits the egress of IPsec traffic and AO-approved control plane traffic. The internal interface of the Inner VPN Gateway is configured to only permit traffic with an IP address and port associated with Red network services.

The Inner VPN Gateway cannot route packets between Red and Gray networks, any packets received on a Red network interface and sent to a Gray network interface must be transmitted within an IPsec VPN tunnel that is configured according to this CP. The Inner VPN Gateway, selected from the CSfC Components List, must be physically separate from the Gray firewall and inner firewall.

5.6.2 INNER TLS-PROTECTED SERVER

The Inner TLS-Protected Server(s) utilizes TLS with select cryptographic cipher suites to provide confidentiality, integrity, and mutual authentication between a TLS EUD and TLS-Protected Server(s). The TLS-Protected Server is located between the gray firewall and the inner firewall. The MA CP allows the TLS-Protected Server to utilize any protocol that is encapsulated within TLS.

The TLS Protected Server should have a different cryptographic library from the one used in the Outer VPN Gateway and may only be managed by the Red Management Services.

The TLS-Protected server can be managed externally, through a dedicated network management interface, or internally, through a trusted inline interface. If the TLS Protected Server is managed from the internal interface, the host-based firewall must be configured to allow only those ports and protocols that are required for the solution to operate as specified in this CP (see Section 12.7). Inner TLS-Protected Servers must be managed from the red administration workstation. The TLS Protected Server also are configured with a host-based firewall. The host-based firewall must have a deny-by-default rule set for both inbound and outbound data plane, control plane, and management traffic. Only ports and protocols that are required for the system to operate, have an explicit allow enabled in the firewall.

Examples of TLS-Protected Servers include, but are not limited to, web servers, SIP servers, Virtual Desktop Infrastructure (VDI) Servers, and Mobile Device Management (MDM) servers. Web servers implemented as part of the MA CP terminate the inner layer of encryption utilizing HTTPS. SIP servers



Mobile Access Capability Package



utilize SIP over TLS for registration of EUDs and SRTP Endpoints, session setup, and session termination. When SIP servers are included, Session Description Protocol Security Descriptions (SDES) is used over the SIP TLS session for key exchange between TLS EUDs or between a TLS EUD and an SRTP Endpoint. The inner TLS Protected-Server, selected from the CSfC Components List, must be physically separate from the Gray firewall and inner firewall as depicted in Figure 4.

5.6.3 INNER SRTP ENDPOINT

Inner SRTP Endpoints provides cryptographic protection of data in transit. Within the MA solution infrastructure, SRTP Endpoints are located between the Gray firewall and the inner firewall. The inner layer of SRTP encryption can also be terminated between two EUDs (see Section 6.3). Registration, session setup (including authentication and key exchange), and session termination for the SRTP Endpoints is performed utilizing SIP over TLS. Inner SRTP Endpoints are required if supporting TLS EUDs that utilize SRTP.

All SRTP Endpoints that terminate the inner layer of encryption originating from a TLS EUD reside within the CSfC Solution Boundary and must meet all applicable requirements as described in the MA CP.

The VoIP gateway/border controller terminates SRTP Traffic from a TLS EUD and relays the data to the Red network. Inclusion of a VoIP gateway/border controller allows integration with existing enterprise voice systems.

The inner SRTP Endpoint, selected from the CSfC Components List, must be physically separate from the Gray firewall and inner firewall as depicted in Figure 4.

5.7 RED MANAGEMENT SERVICES

Secure Administration of Inner Encryption Components and continuous monitoring of the Red network are essential roles provided by the Red Management Services. Red Management Services are composed of a number of components that provide distinct security to the solution. The MA CP allows flexibility in the placement of some Red Management Services as described below.

5.7.1 RED ADMINISTRATION WORKSTATIONS

The Red administration workstation is responsible for maintaining, monitoring, and controlling all security functionality for the Inner Encryption Components, inner firewall, and all Red Management Service components. The Red administrative workstations are not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services. All MA solutions will have at least one Red administrative workstation. Section 7 provides more detail on management of MA solution components.

5.7.2 RED SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Red SIEMs collect and analyze log data and flow data from the Inner Encryption Components, the inner firewall, and other Red Management Service components. Log data may be encrypted between the



Mobile Access Capability Package



originating component and the Red SIEM with SSHv2, TLS, or IPsec to ensure confidentiality and integrity. The SIEM is configured to provide alerts for specific events.. Customers are encouraged to leverage existing Enterprise SIEM capabilities to monitor log data from Inner Encryption Components, the Inner firewall, and Red Management Services. A Red SIEM may also be utilized to analyze log data from Gray network components when utilized in conjunction with an approved cross domain system (CDS) as described in this CP (see Section 8.5).

5.8 PUBLIC KEY INFRASTRUCTURE COMPONENTS

Mobile Access solutions require PKI services to issue and manage device certificates for Outer VPN Components and Inner Encryption Components. The PKI services consist of an outer CA, Gray Network Certification Revocation Status Services, an inner CA, and Red Network Certification Revocation Services.

5.8.1 OUTER CERTIFICATION AUTHORITIES

An outer CA is required to issue digital certificates for the Outer VPN Components within the solution. These certificates are used for authentication in establishing the outer IPsec tunnels between pairs of VPN Components. The outer CA may also be used to issue WPA2 Enterprise certificates to EUDs for authenticating the WPA2 connection between the EUD and Dedicated Outer VPN (see Section 6.1.1). The outer CA may be an Enterprise CA that is accessible¹ via the Gray or Red network, or a locally-run CA that operates in the Gray or Red network. When an Enterprise PKI capability is utilized, it is managed with that PKI's existing processes and capabilities. Enterprise CAs then provide certificate management services for the MA solution over the Gray or Red network. (See Section 9 for additional details regarding enterprise and locally-run CAs.)

If the outer CA delivers services to, or operates within, the Red network, it is critical to have AO-approved mechanisms in place to transfer any certificate-related information to the Gray network to ensure it is accessible to the Outer VPN Gateway and Gray Management Services. Furthermore, if the outer CA is locally-run, then this CP also requires a physically separate inner CA located in the Red network to issue certificates to the Inner Encryption Components. Physical separation between locally-run CAs is required to comply with the MA CP solution requirement for two security tunnels with independent layers of encryption.

5.8.2 GRAY NETWORK CERTIFICATE REVOCATION STATUS SERVICES

CDPs and OCSP Responders are servers that provide certificate revocation status information to MA solution components. Outer CDPs and OCSP Responders are deployed on the internal side of the Outer VPN Gateway for which outer certificate revocation status information is being made available. Collectively, outer CDPs and OCSP Responders are referred to as Gray Network Certificate Revocation Status Services.

¹ Access to the enterprise PKI may be via a controlled network connection or via a physical interface (e.g., media transfer).



Mobile Access Capability Package



The Gray Network Certificate Revocation Status Services ensure the Outer VPN Gateway can verify the revocation status of the EUD outer certificates used by the Outer VPN Component. The Gray Network Certificate Revocation Status Services may also provide certificate revocation status information to Gray Management Services and to the WPA2 Enterprise Authentication Server when validating EUD EAP-TLS certificates connecting over a Dedicated Outer VPN with wireless connectivity. In some cases, Gray Network Management services may also include an inner CDP (see Section 5.8.4) for EUDs to check revocation status of certificates issued to Inner Encryption Components within the MA solution infrastructure (e.g., TLS-Protected Servers).

Outer CDPs and OCSP Responders are not required components of the MA solution; however, if not utilized, the organization must implement other means, such as whitelists, to ensure revoked certificates are never used to establish the Outer IPsec Tunnel, a tunnel for Gray Management Services, or a WPA2 connection between an EUD and a dedicated outer VPN.

5.8.3 INNER CERTIFICATION AUTHORITIES

An inner CA is required to issue digital certificates for the Inner Encryption Components in the solution. These certificates are used for authentication in establishing the inner IPsec or TLS tunnels between pairs of Inner Encryption Components. The inner CA may be an enterprise CA that is accessible via either the Red network or a locally-run CA that operates within the Red network. (See Section 9 for additional details regarding enterprise and locally-run CAs.) When an Enterprise PKI capability is utilized, it is managed with that PKI's existing processes and capabilities. Enterprise CAs then provide certificate management services for the MA solution over the Red network.

5.8.4 RED NETWORK CERTIFICATE REVOCATION STATUS SERVICES

Inner CDPs and OCSP Responders are located either between the Inner Encryption Components and inner firewall, or on the internal side of the inner firewall. Inner CDPs and OCSP Responders make certificate revocation status information available to Inner Encryption Components of the solution infrastructure. Collectively, inner CDPs and OCSP Responders are referred to as Red Network Certificate Revocation Status Services.

The Red Network Certificate Revocation Status Services ensure the solution infrastructure Inner Encryption Components can verify the status of the inner certificates used by the EUDs. The Red Network Certificate Revocation Status Services may also provide certificate revocation status information to Red Management Services.

Inner CDPs and OCSP Responders are not required components of an MA solution, but if not utilized then the organization must implement other means, such as whitelists, to ensure revoked certificates are never used to establish either the Inner Security Tunnel or a tunnel for Red Management Services.



Mobile Access Capability Package



6 END USER DEVICE COMPONENTS

The MA CP supports both VPN EUDs and TLS EUDs; however, the EUD must be dedicated as either a VPN EUD or TLS EUD. VPN and TLS EUDs are composed of a computing device and optionally include a physically separate Dedicated Outer VPN to provide the outer layer of IPsec encryption. When a Dedicated Outer VPN is included as part of the EUD it must either be physically connected to the computing platform utilizing an Ethernet cable or connected over WiFi with WPA2.

An RD is required when connecting to the Black network, except for the solution designs and use cases specified in Section 4.1.3 and 6.1.1.

6.1 OUTER VPN COMPONENT

The allowable Outer VPN Components for both the VPN and TLS EUD are identical. Authentication of peer VPN Components and cryptographic protection of data in transit are fundamental aspects of the security provided by the EUD Outer VPN Component.

The Outer VPN Component establishes an IPsec tunnel with the solution infrastructure Outer VPN Gateway, which provides device authentication, confidentiality and maintains the integrity of information traversing Black networks. The MA CP allows the use of VPN Gateways or VPN Clients to be utilized as the Outer VPN Component of EUDs.

The private keys and certificates utilized for the authentication of the Outer VPN Component are considered Controlled Unclassified Information (CUI) and must be protected with a FIPS 140-2-validated cryptographic module. Customers deploying MA solutions in high-threat environments may also choose to implement controls to mitigate against tampering attacks.

Solutions supporting Multiple Security Levels (as described in Section 4.2.4) configure EUDs to perform authentication of the outer IPsec tunnel utilizing an EAP-TLS session to the Outer VPN Gateway. Mutual authentication occurs between the EUD and the Authentication Server utilizing the Outer VPN Gateway as an EAP pass-through.

6.1.1 DEDICATED OUTER VPN

A Dedicated Outer VPN can be utilized as the Outer VPN Component for EUDs. Utilizing a physically separate VPN as part of the EUD improves security by providing physical separation between the computing device and the outer layer of encryption. When a Dedicated Outer VPN is used as part of an EUD, there is no requirement to utilize a Government RD (see Appendix D. End User Device Implementation Notes). When utilizing a Dedicated Outer VPN, the outer VPN and computing device are collectively referred to as the EUD.

The Dedicated Outer VPN included as part of the EUD must either be physically connected to the computing platform utilizing an Ethernet cable or connected over WiFi with WPA2. The WiFi connection between the computing platform and Outer VPN Gateway can be either WPA2 Enterprise or WPA2 PSK



Mobile Access Capability Package



(see Section 9.3 for requirements). The Dedicated Outer VPN is selected from either the *IPsec VPN Gateway* section or the *IPsec VPN Client* section of the CSfC Components List. Dedicated Outer VPNs that support wireless connectivity with the computing platform must also be selected from the *WLAN Access System* section of the CSfC Components List.

When a Dedicated Outer VPN is included as part of an EUD, it provides configuration and enforcement of network packet handling rules for the outer layer of encryption. The configuration settings of the Dedicated Outer VPN may need to be updated when entering new environments (e.g., updating the Default Gateway). Dedicated Outer VPNs are dedicated to a single security level and can only provide the outer layer of IPsec for clients connecting to a Red network of the same security level.

6.1.2 OUTER VPN CLIENT

An Outer VPN Client can be utilized as the Outer VPN Component for MA EUDs. The purpose of the Outer VPN Client is to establish an IPsec tunnel to the Outer VPN Gateway of the MA solution infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client, and the Operating System on which it is installed on the computing platform, is responsible for providing configuration and enforcement of network packet handling rules for the Outer layer of encryption. The Outer VPN Client is selected from the *IPSec VPN Client* section of the CSfC Components list. The VPN Client is installed on the computing device selected from the *Mobile Platform* section of the CSfC Components List.

6.2 VPN EUD

VPN EUDs utilize IPsec using a VPN Client to provide the Inner layer of encryption. The purpose of the Inner VPN Client is to establish an IPsec tunnel to the Inner VPN Gateway of the MA solution infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process, following establishment of the outer VPN tunnel. Once the Inner VPN Client establishes the inner IPsec tunnel, any application installed on the computing device can send and receive classified data with the Red network.

The private keys and certificates utilized for the authentication of the Inner VPN Component are considered CUI and must be, at a minimum, protected by enabling the native platform DAR protection.

Appendix D. End User Device Implementation Notes provides more detail on the allowable configuration of VPN EUDs.

A VPN Client can be utilized as the Inner VPN Component for VPN EUDs. The purpose of the Inner VPN Client is to establish an IPsec tunnel to the Inner VPN Gateway of the MA S

olution Infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client and the Operating System on which it is installed is responsible for providing configuration and enforcement of network packet handling rules for the Inner



Mobile Access Capability Package



layer of encryption. The Inner VPN Client is selected from the *IPSec VPN Client* section of the CSfC Components list. The VPN Client is installed on the computing device selected from the *Mobile Platform* section of the CSfC Components List.

Virtualization must be utilized when an Outer VPN Client and Inner VPN Client both reside on the same computing device. The virtualization ensures that two separate IP stacks are utilized. The MA CP allows for Type 1 or Type 2 Hypervisors to be utilized to provide logically separated operating systems, each with their own IP stack.

6.3 TLS EUD

TLS EUDs utilize TLS clients or SRTP clients to provide the inner layer of encryption. The inner layer of TLS or SRTP is implemented by TLS clients and SRTP clients provided by individual applications installed on the computing device. Each application that sends and receives data to the Red network must be selected and configured in accordance with the requirements of the CP. Each application then terminates the inner layer of encryption to TLS-Protected Servers and SRTP Endpoints within the MA solution infrastructure.

The private keys and certificates utilized for user authentication of the inner TLS and SRTP clients are determined by the AO. If the private keys and certificates are considered CUI then the EUD component must, at a minimum, implement the native platform encryption. If the private keys and certificates are considered to be classified, then the EUD must be treated as classified at all times or implement an NSA-Approved DAR Solution (see Section 4.2.1).

TLS EUDs must use either a Government RD or dedicated outer VPN to connect to the Black network, except for the use cases defined in Section 4.1.3 provides more detail on the allowable configuration of TLS EUDs.

6.3.1 TLS CLIENT

Applications with a TLS client can be installed on the computing device and utilized for the Inner layer of TLS encryption. On TLS EUDs, every application that sends or receives data through the Outer VPN Component must be independently. For example, if a Voice Application, Web Browser, MDM Agent, and Email Client are installed on the computing device, each application is configured to establish a TLS session to the TLS-Protected Server in the MA solution infrastructure. In some instances an application may perform both TLS and SRTP encryption. Those applications must be configured to meet requirements for both TLS clients and SRTP clients.

The TLS-client utilizes a device certificate or user certificate for authentication to the TLS-Protected Server. The certificates are issued by the inner CA, which may be the same CA that issues certificates to the TLS-Protected Servers (e.g., customer enterprise CA). When a device certificate is used, the user must then authenticate to the Red network before gaining access to any classified data (e.g., username and password, token). When a user certificate is used, the user certificate authenticates the inner layer



Mobile Access Capability Package



of TLS encryption and authenticates the user for access to the requested classified data. A combination of the TLS Client and Computing Device Operating System is responsible for providing configuration and enforcement of network packet handling rules for the Inner layer of encryption.

6.3.2 SRTP CLIENT

Applications with an SRTP client can be installed on the computing device and utilized for the inner layer of SRTP encryption. If multiple SRTP clients are installed on the TLS EUD, then each must be configured independently. SRTP Clients are generally used to encrypt real time traffic, such as voice or video. In some instances, an application may perform both TLS and SRTP encryption. Those applications must be configured to meet requirements for both TLS clients and SRTP clients.

SRTP clients utilize certificates for mutual authentication. In most cases, the SRTP-client utilizes a user certificate for authentication. User certificates are issued by the same PKI that issues certificates to TLS Protected Servers (e.g., customer enterprise PKI), which may be different than the inner CA.

Alternatively, the SRTP client can utilize a device certificate for authentication followed by user authentication (e.g., username and password, token, smartcard, etc.). A combination of the SRTP Client and Computing Device Operating System is responsible for providing configuration and enforcement of network packet handling rules for the Inner layer of encryption.

7 MOBILE ACCESS CONFIGURATION AND MANAGEMENT

The MA CP includes design details for the provisioning and management of Solution Components. The following sections describe the design in detail and Section 12 articulates specific configuration requirements that must be met to comply with the MA CP.

7.1 SOLUTION INFRASTRUCTURE COMPONENT PROVISIONING

Provisioning is an out-of-band process performed in a physically secured area (e.g., the Red network) through which MA solution infrastructure components are configured and initialized before their first use. During the provisioning process, the security administrator configures the Outer VPN Gateway, Gray Management Services, Inner Encryption Components, and Red Management Services in accordance with the requirements of this CP.

During provisioning, the Outer VPN Gateways and Inner Encryption Components generate a public/private key pair and output the public key in a Certificate Signing Request (CSR). The security administrator delivers the Outer VPN Gateways' CSR to the outer CA and the Inner Encryption Components' CSR to the inner CA. The appropriate CA processes the CSR for each encryption component and returns a signed X.509 certificate. The security administrator then installs the unique signed certificate and the certificate chain, which consists of the signing CA's certificate and the Trust Anchor certificate (i.e., Root CA certificate). The security administrator may also install an initial CRL.



Mobile Access Capability Package



7.2 EUD PROVISIONING

Provisioning is an out-of-band process performed in a physically secured area (e.g., the Red network) through which MA EUDs are initialized before their first use. During the provisioning process, the security administrator loads and configures the required software for the EUD. The security administrator instructs the EUD to generate the requisite public/private key pairs for the EUD's Outer VPN Component and Inner Encryption Component as well as output the public keys in a specified CSR format for delivery to the outer CA and the inner CA, respectively.

If the VPN EUD utilizes a dedicated outer VPN to establish the outer IPsec tunnel, the public/private key pairs and CSRs are generated on and output from the dedicated outer VPN device. For TLS EUDs that require an enterprise user certificate, the CSR is delivered to the CA in the customer's organization that has the authority to issue enterprise user certificates. This CA may not be the same as the inner CA.

If the EUD cannot generate its own key pairs or CSRs, then a dedicated management workstation is required to generate the key pairs for the EUD and construct the CSRs for delivery to the outer CA and the inner CA. The CAs process the CSRs and return signed certificates to the Security Administrator, who installs the certificates onto the EUD, and if required, the Dedicated Outer VPN device. If required, the Security Administrator also installs the private keys onto the EUD. The Security Administrator then finalizes the security configuration of the EUD before it used for the first time.

If the MA solution owner is unable to remotely manage EUDs over the two layers of encryption within an MA solution, then the EUDs must be periodically re-provisioned in order to receive software and configuration updates. Re-provisioning consists of revoking the EUD's existing certificates and provisioning the EUD using a trusted baseline configuration that does not make use of any retained data originally stored on the EUD (e.g., factory reset and provision as a new device). This CP does not impose a particular frequency for re-provisioning. Without remote management of EUDs, re-provisioning is the only means of applying security-critical patches to EUDs..

Due to the time and effort needed to re-provision EUDs, it is preferable to remotely manage them when possible. With remote management capabilities, updated software and configuration data can be provided from a central management site through the MA solution to the EUD after the EUD establishes the two MA solution tunnels (see Section 12.13).

7.3 ADMINISTRATION OF MOBILE ACCESS COMPONENTS

Each component in the solution has one or more administration workstations that are responsible for maintaining, monitoring, and controlling all security functions for that component. It should be noted that all of the required administrative functionality does not need to be present in each individual workstation, but the entire set of administration workstations must collectively meet administrative functionality requirements.



Mobile Access Capability Package



The administration workstation is used for configuration review and management. Implementations will employ a SIEM in the Gray Management Services for log management of Gray Infrastructure Components except where AOs utilize a CDS to move Gray network log data to a Red SIEM.

Given the architecture of the solution, each layer has its own distinct administration LAN or VLAN; the Inner Encryption Components are managed from the Red Management Services and the Outer VPN Gateway and supporting components are managed from the Gray Management Services.

The Gray administration workstation, along with all Gray Management Services, is physically connected to the Gray firewall. The Gray firewall maintains separate ACLs to permit management traffic to/from the Gray Management Services, but prohibits such traffic from all other components. These ACLs ensure that approved management traffic is only capable of flowing in the intended direction. This architecture provides the separation necessary for two independent layers of protection.

Administration workstations must be dedicated terminals for the purposes given in the CP. For example, administration workstations are not to be used as the registration authority for the CA, a SIEM, or as a general user workstation for performing any functions besides management of the solution. Additionally, Administration workstations cannot be used as an enrollment workstation or provisioning workstation.

Management of all MA solution components is always encrypted to protect confidentiality and integrity, except in the case where components are locally managed through a direct physical connection (e.g., serial cable from Gray administration workstation to Outer VPN Gateway). Management traffic must be encrypted with SSH, TLS, or IPsec. When components are managed over the Black network, a CSfC Solution must be implemented in order to provide two layers of approved encryption. This requirement is not applicable if the MA solution infrastructure components are being managed from the same LAN or VLAN. For example, a Gray administration workstation residing within the Gray Management Services at the same site as the Outer VPN Gateway need not use CNSA Suite algorithms since this traffic does not traverse an untrusted network.

In most cases, mobile platforms are managed over the Black network by utilizing the outer layer of IPsec and an MDM server selected from the CSfC Components List. When an MDM server is used to manage TLS EUDs, the MDM server is considered a TLS-Protected Server and the MDM agent is considered a TLS Client. As a result, the MDM server must be placed between the Gray firewall and inner firewall. Like other Inner Encryption Components, the MDM server is managed from the Red administration workstation. As a TLS-Protected Server, the MDM server must be configured to establish a session with the MDM agent in accordance with the requirements in Table 16. Although not mandatory, the use of an MDM enables organizations to dynamically change policies enforced on the mobile platform, allowing more flexibility. Additionally, there are several security advantages by using an MDM including the ability to perform a remote wipe of the EUD.



Mobile Access Capability Package



7.4 EUDS FOR DIFFERENT CLASSIFICATION DOMAINS

As specified in this CP, an EUD is only authorized to communicate with Red networks operating at the same classification level. However, it does not preclude the possibility that an approved CDS can be used within an infrastructure to provide cross domain transfer of data between EUDs operating at differing classification levels. It also does not preclude the use of an EUD as an access CDS for multiple enclaves operating at different classification levels if approved through the appropriate CDS approval process.

The requirements for a CDS capable of providing separation between enclaves of two or more classification levels are outside the scope of this CP. If developing an MA solution with a CDS capability, the solution must register against this CP and utilize the appropriate CDS approval processes.

8 CONTINUOUS MONITORING

The MA CP allows customers to utilize EUDs physically located outside of a secure government facility. With this increase in accessibility comes a need to continuously monitor network traffic and system log data within the solution infrastructure. This monitoring allows customers to detect, react to, and report any attacks against their solution. This continuous monitoring also enables the detection of any configuration errors within solution infrastructure components.

At a minimum, this CP requires an auditor to review alerts, events, and system logs on a weekly basis. This minimum review period allows customers in tactical environments to implement solutions in situations where it may not be feasible to perform real-time monitoring. Operational and strategic implementations of the MA solution, however, should have an auditor review alerts, events, and system logs on a much more frequent basis and in many cases are recommended to leverage Operations Centers to perform continuous monitoring of the solution.

8.1 MONITORING POINTS

The MA CP requires network traffic monitoring occur, at a minimum, in two of the four listed areas within the solution infrastructure. Network traffic can be monitored using an IDS; however, it is preferable to utilize an IPS to enable real-time responses. While it is only required to monitor two of the four locations, customers monitoring all four points have the best visibility, enabling maximum detection of malicious activity or misconfiguration of components.



Mobile Access Capability Package

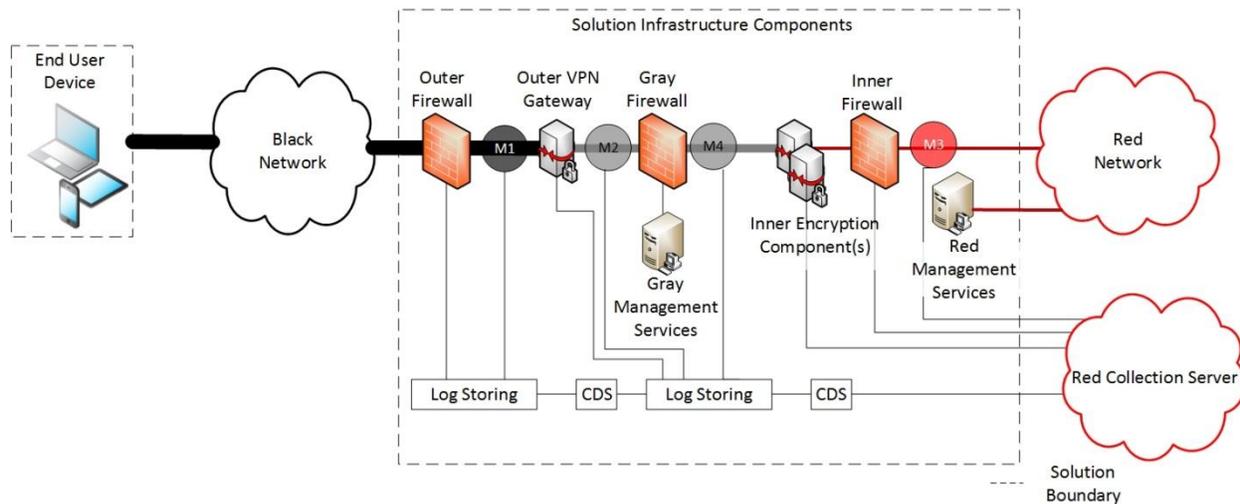


Figure 7. MA Solution Continuous Monitoring Points

Figure 7 depicts the four locations that customers must choose from when implementing network monitoring capabilities. There are multiple configurations for deploying the IDS/IPS at two or more of the monitoring points (M1, M2, M3, and M4) listed in this CP. IDS/IPS systems can ingest traffic from network taps, span ports, or in-line with the solution.

The following paragraphs define each of the four monitoring points. These descriptions outline the analysis and alerts that would be generated by the IDS/IPS in each location. If a customer decides to implement an IPS, then it should be configured to block specific traffic flows as well as generate an appropriate alert.

Monitoring Point 1 (M1): Located between the outer firewall and Outer VPN Gateway, an M1 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the outer firewall. These alerts indicate a failure of the outer firewall’s filtering functions and are evidence of either an improper configuration or a potential compromise. Normal traffic at M1 is well-defined (e.g., IPsec encryption and a limited number of approved control plane protocols) and, as a result, is unlikely to produce false positives. Since nearly all traffic traversing M1 is encrypted with IPsec, the IDS/IPS is limited to analyzing only IP addresses, ports, protocols, and flow data. Management of the M1 IDS/IPS occurs within the Black network.

Monitoring Point 2 (M2): Located between the Outer VPN Gateway and Gray firewall, an M2 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the Outer VPN Gateway. These alerts can indicate a failure of the outer firewall or outer VPN’s filtering functions and are evidence of either an improper configuration or a potential compromise. Normal traffic at M2 is not as narrowly defined, but includes IPsec traffic, data plane traffic encrypted with TLS or SRTP, control plane traffic, and management traffic. Nearly all traffic traversing



Mobile Access Capability Package



M2 is encrypted either with IPsec, TLS, SRTP, or SSH, which prevents deep packet inspection. Management of the M2 IDS/IPS occurs within the Gray Management Services.

Monitoring Point 3 (M3): Located between the inner firewall and Red network, an M3 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the inner firewall. These alerts indicate a failure of the inner firewall's filtering functions. Of the four monitoring points, M3 is the most difficult to define, but in many implementations, utilizing M3 allows for deep packet inspection as traffic may not be encrypted. Management of the M3 IDS/IPS occurs from within the Red Management Services.

Monitoring Point 4 (M4): Located between the Gray firewall and Inner Encryption Components, an M4 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the Gray firewall. These alerts indicate a failure of the Gray firewall's filtering functions and are evidence of either an improper configuration or a potential compromise. Management of the M4 IDS/IPS occurs from within the Gray Management Services.

Monitoring Multiple Points: Although the MA CP only requires monitoring two of the four points, customers are encouraged to monitor all four locations (see Section 12.14). Implementation of four separate components to monitor each point ensures that malicious traffic cannot inadvertently be transferred to the Red network.

Movement of network traffic from M3 to the Gray or Black network is explicitly prohibited. Additionally, movement of network traffic from M2 and M4 to the Black network is explicitly prohibited. The advantages of consolidated monitoring at all four points are fully realized when data from all devices is collected within the Red monitoring enclave using a CDS (see Section 8.5) and event correlation (see Section 8.6).

8.2 LOG DATA

The MA CP requires the implementation of a SIEM component within the Gray Management Services except in instances where an approved CDS is used to transport Gray security data to a Red SIEM. The Gray SIEM collects, aggregates, correlates, and analyzes security data from Gray Management Components, the outer VPN, and Gray firewall. The SIEM also provides alerts to auditors when anomalous behavior is detected.

The Gray SIEM is not permitted to collect logs from the outer firewall or M1 unless utilized in conjunction with an approved CDS. To protect the confidentiality and integrity of the data, all logs sent to the SIEM should be encrypted with TLS, SSH, or IPsec.



Mobile Access Capability Package



8.3 NETWORK FLOW DATA

Network flow data (e.g., NetFlow, J-Flow, NetStream) is generated from network devices (e.g., routers, switches and standalone probes) and can be analyzed to provide a picture of network traffic flow and volume. Network flow data consists of IP protocols, source and destination IP addresses, and source and destination ports.

Monitoring network flow data requires establishing a baseline and updating it on a consistent basis. Network flow data should be reviewed regularly for systems generating excessive amounts of traffic, systems trying to connect to improper IP addresses, and systems trying to connect to closed ports on internal servers.

Network flow data can be collected from any network within the solution infrastructure. Network flow data from the Black network can be collected from the outer firewall and sent to a Black network collection server. Network flow data from the Gray network must be collected from the Outer VPN Gateway or Gray firewall and sent to a collection server in the Gray Management Services. Finally, network flow data can be collected from the Red inner firewall and sent to a collection server on the Red network.

To maximize the effectiveness of collecting flow data from multiple network segments, all data should be centralized within the Red monitoring enclave for ingest into a single SIEM solution. Section 8.5 below outlines the various use-cases for implementing an approved CDS to move Black and Gray data to the Red network.

8.4 CHANGE DETECTION

One method of automating the detection of configuration changes without the complexity and expense of dedicated configuration management systems is to leverage the collection of syslog. In addition to collecting basic security events, the syslog facility is also capable of sending events related to system configuration changes. Queries, which generate alerts for administrators and auditors to review, can be developed on either the log collection server or the SIEM.

8.5 COLLECTION

This section provides a description of the primary sources for security event data and the recommended procedure for collecting data from the solution infrastructure.

Security event data includes, but is not limited to, syslog, IDS/IPS alerts, and network flow data. The syslog facility can be very broad and include security relevant events, configuration changes, health and status alerts, and other data which(that?) may prove useful when assembling the overall status of the security posture of a system. To protect the confidentiality and integrity of the data, all feeds should be encrypted with SSH, TLS, or IPsec.



Mobile Access Capability Package



Black Network Segment – The two key components within the Black network segment are the outer firewall and the optional M1 monitoring point. The recommended solution would receive data from both devices on a single data collection server and forward this data to the Gray collection server through an approved CDS.

Gray Network Segment – The key components within the Gray network segment are the outer VPN, Gray firewall, the required M2 monitoring point, the optional M4 monitoring point, and the associated Gray Management Services.

This CP requires, at a minimum, that security data be sent directly to a SIEM located within the Gray network. The Gray SIEM may receive data feeds from a central data collection server, as depicted in Figure 7. The Gray SIEM is not permitted to collect data from the Black network segment unless an approved CDS is used.

The recommended solution would receive data from all devices on a single data collection server and forward this data to the Red collection server through an approved CDS.

Red Network Segment – The key components within the Red network segment vary based upon the services offered to EUDs, but must, at a minimum, include the inner firewall and the required M3 monitoring point. All security event data must be sent to a single collection server located within the Red monitoring enclave and may be fed into the Red SIEM solution; however, the Red SIEM is permitted to receive data flows directly from the Red components.

The recommended solution utilizes the Red SIEM to collect, aggregate, correlate, and analyze security data from all three boundaries (i.e., Black, Gray, and Red). The Red SIEM is not permitted to collect data from the Black or Gray segments unless an approved CDS is used.

8.6 CORRELATION

In order to support correlation of data from the Black, Gray, and Red components, the MA CP allows for the use of an approved CDS to feed the lower boundaries into the Red enclave. A Red SIEM should be located within an enclave protected from the larger enterprise of the Red network (see Section 12.14).

9 KEY MANAGEMENT

MA solutions utilize asymmetric algorithms (as defined in Table 8 - Table 11) and X.509 certificates for component authentication to establish the outer and inner encryption tunnels. Each MA solution component contains a private authentication key and a corresponding public certificate issued by an authorized CA. In addition, a trusted CA certificate is installed, as well as any other CA signing certificates that connect to the trusted CA, so that a trusted certificate chain is established between the Component certificate and the trusted CA certificate. Each MA solution infrastructure component should also contain the required CRLs to support revocation status checking of component certificates. If CRLs are



Mobile Access Capability Package



not used, other mechanisms can be implemented (e.g., whitelists) in MA solution infrastructure components.

It is preferable for the authentication keys (public/private key pair) to be generated on the security component, where the private keys are never exported out of the component. If the component cannot generate its own key pair, a dedicated management workstation is required to generate the key pair for the component. The public keys are sent in certificate requests to the outer and inner CAs that create and sign authentication certificates containing the public keys. If the request is for a user certificate, the request is delivered to the CA in the customer's organization that has the authority to issue enterprise user certificates. This CA may not be the same as the inner CA. The authentication certificates are delivered to, and installed on, the security components during provisioning, along with the private keys if they were not generated on the component. The CAs also issue signed CRLs to provide revocation status information for the certificates issued by the CAs. CRLs are transferred to CDPs or OCSP Responders as discussed in Section 9.1, where the certificate revocation status information is made available to MA Solution Infrastructure Components.

To provide confidentiality services within MA solutions, the components utilize key agreement protocols (such as Elliptic Curve Diffie-Hellman(ECDH)) to generate ephemeral encryption keys. The use of ephemeral encryption keys is not part of key management discussed in this section, as CAs are not required in issuing and managing these keys.

The CAs that issue authentication certificates to MA solution components operate either as Enterprise CAs (e.g., DoD PKI, KMI, and Agency PKI) or locally run CAs. Existing Enterprise CAs should be used whenever possible, as the advantages for using these CAs outweigh those associated with locally run CAs. Enterprise CAs have established operations, as well as Certificate Policies and Certification Practices Statements (CPSs) that customer organizations can leverage for their MA solution. These Enterprise CAs operate at Federal Department (e.g., DoD PKI, KMI) and Agency levels, and offer wide-scale interoperability across MA solutions (i.e., the certificate policies and their registered policy OIDs are widely accepted across the Federal Department or Agency). When an Enterprise Root CA is utilized, the MA CP requires that at least two existing Subordinate CA's are used to issue certificates. One Subordinate CA issues certificates to Outer Encryption Components (known as the outer CA) and the other CA is utilized to issue certificates to Inner Encryption Components (known as the inner CA). To ensure that the same certificate cannot be used for authenticating both the outer and inner tunnels, the outer CA and inner CA are used as trust anchors to validate the outer tunnel and inner tunnel authentication certificates, respectively.

For MA solutions requiring interoperability across a Federal Department, the Department-level Enterprise CAs should be leveraged. Examples of Department-level Enterprise CAs include the DoD PKI; the NSA Key Management Infrastructure (KMI); the National Security Systems (NSS) PKI; the Intelligence Community (IC) PKI; the Department of Homeland Security (DHS) PKI; and the Department of Energy (DoE) PKI. Enterprises like this leverage Department-level Trusted CAs which reside under the same Root



Mobile Access Capability Package



CA. Trusted CAs like this can be used as trust anchors in multiple MA solutions throughout a Federal Department, thereby providing certificate trust interoperability across those MA solutions. In addition, certificates issued by Department-level Enterprise CAs may assert registered policy OIDs that are acceptable for use through the Federal Department. A user with a MA EUD provisioned with certificates from a Department-level Enterprise CA could possibly use their EUD in many different MA solutions deployed throughout a Federal Department.

Similarly, MA solutions requiring interoperability across a Federal Agency should leverage Agency-level Enterprise CAs. Agency-level Enterprise CAs issue certificates only to Agency personnel and Non-Person Entities (NPEs). Enterprises leverage Agency-level Trusted CAs which resides under the same Root CA. Trusted CAs can be used as trust anchors in multiple MA solutions throughout that Agency. Furthermore, certificates issued by Agency-level Enterprise CAs may assert registered policy OIDs that are acceptable for use through the Federal Agency. A user with a MA EUD provisioned with certificates from an Agency-level Enterprise CA could possibly use their EUD in different MA solutions deployed throughout that Federal Agency.

For both types of Enterprise CAs described above, an MA solution owner could deploy and operate independent subordinate CAs that are issued certificates by a higher-level Enterprise CA. The benefit of this configuration is that it allows tailoring of the subordinate CA operations to the local environment without losing the interoperability benefits gained by leveraging Enterprise CAs. However, the MA solution owner is responsible for defining and implementing CPSs for the Subordinate CAs that are approved by the Enterprise CA policy authorities.

Finally, MA solutions requiring minimal or no interoperability can deploy and operate their own locally run CAs that are independent of any Enterprise CAs. In this configuration, certificate policy and interoperability is constrained to the specific MA solution. Furthermore, the MA solution owner is required to develop and maintain CPSs that detail the operational procedures for the locally run CAs. In addition, the customer may need to develop and maintain a higher-level Certificate Policy if one does not already exist.² Table 3 summarizes the differences between Enterprise and locally run CAs.

Table 3. Certificate Authority Deployment Options

CA Type	Certificate Policy	Interoperability	Operations
Department-level Enterprise	Owned and managed at the Department level (e.g. DoD PKI, NSA KMI, NSS PKI, IC PKI, DHS PKI, DoE PKI)	Department-wide	Performed by the Enterprise

² CNSSP 25 is the governing policy for PKI solutions in support of Secret MA solutions. For MA solutions that are higher than Secret, the MA solution owner is required to develop a Certificate Policy that is approved by the local Approving Official (AO).



Mobile Access Capability Package



CA Type	Certificate Policy	Interoperability	Operations
Agency-level Enterprise	Owned and managed at the Agency level	Agency-wide	Performed by the Enterprise
Subordinate CA (Enterprise)	Owned and managed at the Department or Agency level	Department-wide or Agency-wide	Performed by the Enterprise and the MA solution owner
Locally run (Non-Enterprise)	Owned and managed at the MA solution level	Constrained to the MA solution	Performed by the MA solution owner

In all CA configurations identified above, outer CAs issue and manage authentication certificates for Outer VPN Components and Gray Management Service Components; inner CAs, and optionally existing CAs that support enterprise services, issue and manage authentication certificate for Inner Encryption Components and Red Management Service Components. Outer CAs can be included as either part of the Gray network or Red network. Inner CAs, including existing enterprise CAs, can only be located in the Red network.

To assist the CAs in their operations, the CAs may communicate with management services (e.g., Device Managers (DMs)) deployed in the corresponding network to support enrollment and life-cycle certificate management for MA Solution Components. Outer and inner CAs in the Red network are limited to directly communicating with Red Management Services. Outer CAs in the Gray network are limited to directly communicating with Gray Management Services. When the CA is not located in the same network as the required management services, an AO-approved CDS may be utilized allowing indirect communication (for example Certificate Enrollment). The Red and Gray Management Services enable the certificate request/response process between an MA solution component and a CA. This CP recommends provisioning of MA solution components in the Red network, and that all enrollment and life-cycle certificate management be performed in accordance with the applicable Certification Practices Statements (CPSs).

This solution utilizes device authentication certificates and, in some instances, user authentication certificates. Device certificates and private keys used in the solution are considered CUI (unless determined to be higher by the AO) because they are only used for mutual authentication, not for traffic encryption or granting access to classified data. User private keys are classified to the level determined by the AO (often treated as classified to the level of the Red network). While the CP enables AOs to define the classification level of User and Device private keys, the allowable options for use and handling of EUDs is dependent on that classification. If any of the private keys stored on an EUD are considered classified, then the solution must be treated as classified at all times or implement a NSA approved DAR Solution.

Thus, an out-of-band method must be used to issue the initial certificates to the Components. Subsequent rekeying, however, should take place over the network through this solution prior to the current key's expiration (see Section 9.2 for additional details regarding over-the-network remote



Mobile Access Capability Package



certificate rekey). The key validity period for certificates issued by locally run CAs cannot exceed 14 months, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to CRLs are distributed to Gateways within 24 hours of CRL issuance.

9.1 DISTRIBUTION OF CERTIFICATE REVOCATION LISTS

Certificate Revocation Lists (CRLs) are used by CAs to convey the revocation status of certificates issued by those CAs, and those CRLs need to be made available to the MA solution components.

A CRL Distribution Point (CDP) is a web server whose sole function is to provide external distribution of, and access to CRLs issued by CAs. CDPs do not serve any other content, and, in particular, do not host any dynamically generated content. CDPs also do not provide any other services other than the distribution of CRLs. CDPs are optional in an MA solution, and they can exist in the Gray or Red networks. The Outer VPN Gateway in the solution infrastructure accesses an outer CDP, located in the Gray network, to obtain CRLs and check revocation status of EUD Outer VPN Components prior to establishing the outer encryption tunnel. Furthermore, a CDP operating in the Gray network can be accessed by Gray Management Service components to obtain CRLs and check the revocation status of the Outer VPN Gateway's certificate prior to establishing a device management tunnel with the Outer VPN Gateway. Finally, a CDP operating in the Gray network can be utilized by the WPA2 Enterprise Authentication Server to check the revocation status of the EUD's WPA2 EAP-TLS certificate prior to the EUD establishing a WPA2 connection to the dedicated outer VPN.

Additionally, the MA CP allows for an inner CDP to be created within the Gray Management Services. Placing an inner CDP in the Gray Management Services allows EUDs to check the certificate status of the Inner Encryption Component prior to establishing a tunnel. To utilize an inner CDP in the Gray Management Services, an AO must determine that CRLs generated by the inner CA are unclassified. These CRLs must also be moved from the Red network to the Gray Management Services using an AO approved method (e.g., CDS).

Inner Encryption Components access an inner CDP, located in the Red network, to obtain CRLs and check revocation status of EUD Inner Encryption Components prior to establishing the inner encryption tunnel. Likewise, a CDP operating in the Red network can be accessed by Red Management Service components to obtain CRLs and check the revocation status of the Inner Encryption Component's certificate prior to establishing a device management tunnel with the Inner Encryption Component.

An outer CDP and an outer CA may reside on the same or different networks. For example, the outer CA may be operated in the Red network, while the outer CDP operates in the Gray network. If they reside on different networks, a one-way transfer mechanism is required to periodically distribute the current CRL from the CA to the CDP. The details and procedures of the one-way transfer mechanism are left to a solution's AO.



Mobile Access Capability Package



As CRLs are digitally signed objects that contain minimally identifying information about MA solution components, there are few concerns with the confidentiality of CRLs. Therefore, CRLs can be downloaded by MA solution components over unencrypted Hypertext Transfer Protocol (HTTP). Furthermore, a CRL's integrity is protected by the digital signature of the CA that issued it, and additional integrity protection during CRL download is not required. Additionally, placement of CDPs on the Gray network for the Outer VPN Gateway and Red network for Inner Encryption Components reduces the exposure to external threat actors.

Use of HTTPS for CRL downloading is discouraged, as it introduces a circular dependency between the CDP and the MA solution component attempting to download the CRL. The MA solution component would need a CRL to determine whether the CDP's certificate is revoked before establishing an HTTPS connection to the CDP. However, the CDP cannot deliver the CRL to the MA solution component until the MA solution component authenticates the CDP by validating its certificate. (Note: Distributing CRLs via HTTP follows the recommendation in Internet Engineering Task Force (IETF) Request for Comments (RFC) 5280 not to use HTTPS to distribute CRLs.)

To provide redundancy and ensure that current CRLs are always made available to MA solution components, multiple outer and inner CDPs may be deployed. The use of multiple CDPs is left to the discretion of the MA solution owner. Furthermore, CDPs may host partition or delta CRLs in addition to complete CRLs. In large MA solutions, the use of partition or delta CRLs can reduce the amount of network traffic needed to distribute updates to CRLs. A CA's Certificate Policy will define whether the use of partition or delta CRLs is permissible.

OCSP Responders or white lists can be utilized in lieu of CDP Servers. OCSP Responders located in the Gray network can provide Certificate Revocation Status information to the Outer VPN Gateway or to the WPA2 Enterprise Authentication Server. Additionally, OCSP Responders in the Red network can provide Certificate Revocation Status information to Inner Encryption Components.

9.2 REMOTE REKEY OF EUD CERTIFICATES

If the EUD is capable of generating its own public/private key pairs and can communicate with the outer and inner CAs using Enrollment over Secure Transport (EST) as defined in IETF RFC 7030, the EUD can have its device certificates remotely rekeyed, as opposed to physically returning the EUD to the provisioning environment as described in Section 7.2. As EST requires a TLS connection to the CA, so that the CA can authenticate an EUD prior to issuing new certificates, it is recommended that the outer and inner CAs both operate in, or be accessible through, the Red network in order to support remote certificate rekey for EUDs. A TLS EUD can therefore utilize its inner TLS tunnel to authenticate to the outer and inner CAs and request certificate rekey. A VPN EUD would need to establish a separate TLS tunnel to the outer and inner CAs after establishing the outer and inner IPsec tunnels.

Once authenticated to the outer and inner CAs, the EUD generates two new public/private key pairs. The newly generated public keys are placed into two new certificate requests in accordance with RFC



Mobile Access Capability Package



7030 – one for the outer tunnel and one for the inner tunnel. The certificate requests are then submitted to the outer and inner CAs for processing using EST. The outer and inner CAs validate that the certificate requests came from a valid and authenticated EUD, process the certificate requests, and return newly signed certificates containing the new public keys to the EUD. The EUD receives and installs the newly rekeyed certificates.

It should be noted that the exact sequence for certificate rekey will vary based on the EUD's implementation of EST. For example, one certificate rekey with one of the CAs may need to be performed first, followed by the second certificate rekey with the other CA.

9.3 WPA2 KEY AND CERTIFICATE MANAGEMENT

As discussed in Section 4.1.3, EUDs can utilize a Dedicated Outer VPN device to establish the outer IPsec tunnel where the computing device connects to the external Dedicated Outer VPN device using a WPA2 connection. WPA2 security is achieved using either Pre-shared Keys (PSKs) or EAP-TLS certificates.

For PSKs, a common PSK with at least 128 bits of security needs to be securely generated, distributed, and installed onto both the computing device and the external Dedicated Outer VPN device. Exposure of the PSK in red form needs to be minimized to the greatest extent possible and only exposed to authorized and trusted personnel responsible for managing and installing the PSK onto the computing device and external Dedicated Outer VPN. Updates to the PSK are to be performed periodically based upon the threat environment. The higher the threat environment, the more often the PSK should be updated.

If WPA2 Enterprise is used, the EUD will require an EAP-TLS certificate to establish the WPA2 connection to the external Dedicated Outer VPN device. This certificate may be issued by the outer CA, or a different CA whose policy supports issuance of WPA2 Enterprise certificates. In either case, issuance of the WPA2 Enterprise certificate should be integrated into the overall provisioning process for the EUD described in Section 7.2. Revocation status information for EAP-TLS certificates issued to EUDs also needs to be made available in the Gray network so that the WPA2 Enterprise Authentication Server can check the revocation status of EUD EAP-TLS certificates (see Section 5.8.2).

10 REQUIREMENTS OVERVIEW

The following five sections (Sections 11 through 15) specify requirements for implementations of MA solutions compliant with this CP. However, not all requirements in the following sections will apply to each compliant solution. Sections 10.1 and 10.2 describe how to determine which set of requirements applies to a particular solution.

10.1 CAPABILITIES

This CP provides the flexibility needed to implement a variety of designs for the implementation of the MA solution. Although most requirements are applicable to all solutions, some requirements are only



Mobile Access Capability Package



applicable to implementations whose high-level designs implement certain features. For example, requirements dealing with TLS EUDs do not include requirements for an Inner VPN Client. Table 4 lists the capabilities covered by this CP and the designators used in the requirements tables to refer to each.

Table 4. Capability Designators

Capability	Designator	Description
TLS Solution	T	Requirement that applies to the MA Solution that connects to the Red network using IPsec as the Outer layer and TLS or SRTP as the inner layer, as described in Section 6.3
VPN Solution	V	Requirement that applies to the MA solution that connects to the Red network using two IPsec tunnels, as described in Section 6.2
TLS Infrastructure	TI	Requirement that applies specifically to the infrastructure associated with the TLS solution
VPN Infrastructure	VI	Requirement that applies specifically to the infrastructure associated with the VPN solution
TLS EUD	TE	Requirement that applies specifically to the EUD associated with the TLS solution
VPN EUD	VE	Requirement that applies specifically to the EUD associated with the VPN solution
All Solution Components	All	Requirement that applies to the EUD and to the Infrastructure, regardless if it is a VPN solution or a TLS solution
CDPs	C	Requirement that applies to the MA Solution that includes CDPs, as described in Section 12.16.4
Multiple Security Levels	MS	Requirement that applies to MA solution infrastructure which supports multiple security levels through the same Outer VPN Gateway
Wireless Connectivity to Dedicated Outer VPN	WC	Requirement that applies to EUDs which include a Dedicated Outer VPN and wireless connectivity to a computing device

Any solution that follows this CP must implement each applicable capability for their solution (e.g., all VPN EUD (V), VPN Infrastructure (VI), and VPN Solution (V) requirements for a solution supporting only VPN EUDs), and may implement multiple capabilities. The “Capabilities” column in the requirements tables in Sections 11 through 15 identifies which capabilities the requirement applies to. A requirement is only applicable to a solution if the “Capabilities” column for that requirement lists one or more of the capabilities being implemented by the solution.

10.2 THRESHOLD AND OBJECTIVE REQUIREMENTS

Multiple versions of a requirement may exist in this CP, with alternative versions designated as being either a Threshold requirement or an Objective requirement:



Mobile Access Capability Package



- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold requirement. However, in these cases, meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible solution owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the “Alternatives” column. Objective requirements that have no related Threshold requirement are marked as “Optional” in the “Alternatives” column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the “Threshold / Objective” column indicates that the Threshold equals the Objective (T=O). Such requirements must be implemented in order to comply with this CP, as long as the requirement is applicable per Section 10.1.

Requirements that are listed as Objective in this CP may become Threshold requirements in a future version of this CP. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this CP.

10.3 REQUIREMENTS DESIGNATORS

Each requirement defined in this CP has a unique identifier consisting of the prefix “MA,” a digraph that groups related requirements together (e.g. KM), and a sequence number (11). Table 5 lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

Table 5. Requirement Digraphs

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 11	Table 6
SR	Overall Solution Requirements	Section 12.1	Table 7
CR	Configuration Requirements for Inner and Outer VPN Components	Section 12.3	Table 12
IR	Inner VPN Component Requirements	Section 12.4	Table 13
OR	Outer VPN Component Requirements	Section 12.5	Table 14
MS	Multiple Security Level Requirements	Section 12.6	Table 15
TE	TLS-Protected Server & SRTP Endpoint Requirements	Section 12.7	Table 16
RD	Retransmission Device Requirements	Section 12.8	Table 17



Mobile Access Capability Package



Digraph	Description	Section	Table
WC	Wireless Connectivity to Dedicated Outer VPN Requirements	Section 12.9	Table 18
EU	End User Device Requirements	Section 12.10	Table 19
PF	Port Filtering Requirements for Solution Components	Section 12.11	Table 20
CM	Configuration Change Detection Requirements	Section 12.12	Table 21
DM	Device Management Requirements	Section 12.13	Table 22
MR	Continuous Monitoring Requirements	Section 12.14	Table 23
AU	Auditing Requirements	Section 12.15	Table 24
KM	Key Management Requirements	Section 12.16	Table 25, Table 26, Table 27, Table 28
GD	Requirements for the Use and Handling of Solutions	Section 13.1	Table 29
	Role-Based Personnel Requirements	Section 14	Table 31
RP	Incident Reporting Requirements	Section 13.2	Table 30
TR	Test Requirements	Section 15.1	Table 32



Mobile Access Capability Package



11 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 6. Product Selection Requirements



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-1	The products used for the Inner VPN Gateway shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	VI	T=O	
MA-PS-2	The products used for any Outer VPN Gateway shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	All	T=O	
MA-PS-3	The products used for any Inner VPN Client shall be chosen from the list of IPsec VPN Clients on the CSfC Components List.	VE	T=O	
MA-PS-4	The products used for any Outer VPN Client shall be chosen from the list of IPsec VPN Clients on the CSfC Components List.	TE, VE	T=O	
MA-PS-5	The products used for the inner and outer CAs shall either be chosen from the list of CAs on the CSfC Components List or the CAs shall be pre-existing Enterprise CAs (e.g. DoD PKI, IC PKI).	VI, TI	T=O	
MA-PS-6	Products used for Mobile Platform EUDs shall be chosen from the list of Mobile Platforms on the CSfC Components List.	VE, TE	T=O	
MA-PS-7	Intrusion Prevention Systems (IPS) shall be chosen from the list of IPS on the CSfC Components List.	VI, TI	O	Optional
MA-PS-8	Products used for the TLS Client shall be chosen from the TLS Client sections (e.g. VoIP Applications, Email Clients, Web Browsers, etc.) of the CSfC Components List.	TE	T=O	
MA-PS-9	Products used for the SRTP Client shall be chosen from the list of VoIP Applications on the CSfC Components List.	TE	T=O	
MA-PS-10	If the solution is using a TLS-Protected Server, it shall be chosen from the list of TLS-Protected Servers on the CSfC Components List.	TI	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-11	If the solution is using an SIP Server, it shall be chosen from the list of SIP Servers on the CSfC Components List.	TI	T=O	
MA-PS-12	If the solution is using an SRTP Endpoint, it shall be chosen from the list of SRTP Endpoints on the CSfC Components List.	TI	T=O	
MA-PS-13	Products used for the outer firewall, Gray firewall, and inner firewall shall be chosen from the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List.	VI, TI	T=O	
MA-PS-14	If the solution is using a MDM, it shall be chosen from the list of MDMs on the CSfC Components List.	VI, TI	T=O	
MA-PS-15	Withdrawn			
MA-PS-16	The Outer VPN Gateway and Inner Encryption Endpoints shall either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	All	T=O	
MA-PS-17	The outer firewall, Outer VPN Gateway, Gray Firewall, Inner Encryption Component, and inner firewall shall use physically separate components, such that no component is used for more than one function (see Figure 1).	VI, TI	T=O	
MA-PS-18	The Outer VPN Gateway and the Inner Encryption Endpoints shall not use the same Operating System. Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity.	VI, TI	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-19	<p>The inner and the outer CAs shall follow one of the following guidelines:</p> <ul style="list-style-type: none">• The CAs come from different manufacturers, where neither manufacturer is a subsidiary of the other.• The CAs are different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.• The CAs utilize an Enterprise PKI approved by the AO.	VI, TI	O	Optional
MA-PS-20	<p>The Gray network firewall and the Inner Encryption Endpoints shall either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.</p>	VI, TI	T=O	
MA-PS-21	<p>The EUD's Outer VPN Component and Inner Encryption Components shall either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.</p>	VE, TE	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-22	The cryptographic libraries used by the inner CA and outer CA shall either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VI, TI	O	Optional
MA-PS-23	The cryptographic libraries used by the Outer VPN Component and the Inner Encryption Components shall either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VE, TE	O	Optional
MA-PS-24	Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRIM for additional guidance).	All	T=O	
MA-PS-25	Components shall be configured to use the NIAP-certified evaluated configuration.	All	O	Optional
MA-PS-26	If the solution supports multiple security levels, the Authentication Server shall be chosen from the list of Authentication Servers on the CSfC Components List.	MS	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-27	If the solution utilizes a Dedicated Outer VPN as part of an EUD, it shall be chosen from the list of IPsec VPN Gateways or IPsec VPN Clients on the CSfC Components List.	VE, TE	T=O	
MA-PS-28	If the solution utilizes a Dedicated Outer VPN as part of an EUD with wireless connectivity to a computing device, the Dedicated Outer VPN shall be chosen from the list of WLAN Access Systems on the CSfC Components List.	WC	T=O	

12 CONFIGURATION REQUIREMENTS

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the MA solution.

12.1 OVERALL SOLUTION REQUIREMENTS

Table 7. Overall Solution Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-SR-1	Network services provided by control plane protocols (such as DNS and NTP) shall be located on the inside network (i.e., Gray network for the Outer VPN Gateway and Red network for the Inner Encryption Endpoints).	VI, TI	T=O	
MA-SR-2	The time of day on Inner Encryption Endpoints, inner firewall, and Red Management Services shall be synchronized to a time source located in the Red network.	VI, TI	T=O	
MA-SR-3	The time of day on the Outer VPN Gateway, Gray firewall, and Gray Management Services shall be synchronized to a time source located in the Gray Management network.	VI, TI	T=O	
MA-SR-4	Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-SR-5	All components shall be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	All	T=O	
MA-SR-6	Solution components shall receive virus signature updates as required by the local agency policy and the AO.	All	T=O	
MA-SR-7	The only approved physical paths leaving the Red network shall be through a MA solution in accordance with this CP or via an AO-approved solution for protecting data in transit. ³	All	T=O	
MA-SR-8	When multiple Inner Encryption Components are placed between the Gray firewall and inner firewall, they shall be placed in parallel.	VI, TI	T=O	
MA-SR-9	Inner Encryption Components shall not perform switching or routing for other Encryption Components.	VI, TI	T=O	
MA-SR-10	Infrastructure components shall only be configured over an interface dedicated for management.	VI, TI	T=O	
MA-SR-11	DNS lookup services on network devices shall be disabled.	All	O	MA-SR-10
MA-SR-12	DNS server addresses on infrastructure devices shall be specified or DNS services shall be disabled.	All	T=O	
MA-SR-13	Automatic remote boot-time configuration services should be disabled (e.g., automatic configuration via TFTP on boot).	All	T=O	

³ In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) product. In particular, it is acceptable for a given site to have both an egress path via an NSA-certified product and an egress path via a CSiC Solution conforming to a CP.



Mobile Access Capability Package



12.2 CONFIGURATION REQUIREMENTS FOR ALL VPN COMPONENTS

Table 8. Approved Commercial Algorithms (IPsec) for up to Top Secret

Security Service	Approved Algorithms	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 FIPS PUB 186-4 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH Group 20) or Diffie-Hellman 3072	NIST SP 800-56A IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460 NIST SP 800-56A
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460



Mobile Access Capability Package



Table 9. Approved Commercial Algorithms (TLS) for up to Top Secret

Security Service	TLS Cipher Suites	Specifications
TLS Cipher Suite (Threshold)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 or TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	FIPS PUB 180-4 FIPS PUB 186-3 FIPS PUB 197 FIPS 800-56A IETF RFC 6460 IETF RFC 5246 IETF RFC 4492
Authentication (Digital Signature)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	
Key Exchange	ECDHE over the curve P-384 (DH Group 20) or Diffie-Hellman 3072	



Mobile Access Capability Package



Table 10. Approved Commercial Algorithms for a Dedicated Outer VPN with Wireless Connectivity

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-128-CCMP (Threshold) AES-256-GCMP (Objective)	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
EAP-TLS Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)	IETF RFC 5216 IETF RFC 5246

Table 11. Approved Commercial Algorithms for up to Top Secret

Security Service	Approved Algorithms	Specifications
Confidentiality (Encryption)	AES-256 in Counter Mode (CM)	IETF RFC 3711 IETF RFC 2675
Integrity	HMAC-SHA1	IETF RFC 3711 IETF RFC 2104
Key Exchange (using SIP Over TLS)	TLS-SDES or DTLS	IETF RFC 4568 IETF RFC 6347



Mobile Access Capability Package



12.3 CONFIGURATION REQUIREMENTS FOR INNER AND OUTER VPN COMPONENTS

Table 12. Configuration Requirements for Inner and Outer VPN Components

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-CR-1	The proposals offered by the Outer and Inner VPN Components in the course of establishing the IKE Security Association (SA) and the ESP SA for inner and outer tunnels shall be configured to only offer algorithm suite(s) containing the Suite B algorithms listed in Table 8.	All	T=O	
MA-CR-2	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any Outer and Inner VPN Component, shall not be used for establishing SAs.	All	T	MA-CR-3
MA-CR-3	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any Outer and Inner VPN Component, shall be removed.	All	O	MA-CR-2
MA-CR-4	Unique device certificates shall be loaded onto the Outer and Inner VPN Gateway along with the corresponding Trust Anchor (signing) certificates.	VI, TI	T=O	
MA-CR-5	A device certificate shall be used for each Outer and Inner VPN Component authentication during IKE.	All	T=O	
MA-CR-6	Authentication performed by Outer and Inner VPN Gateways shall include a check that device certificates are authorized. This check may use a CRL, OCSP, or a whitelist.	VI, TI	T=O	
MA-CR-7	Outer and Inner VPN Component authentication with device certificates shall include a check that certificates are not expired.	All	T=O	
MA-CR-8	Withdrawn			
MA-CR-9	All IPsec connections shall use IETF standards, IKE implementations (RFC 5996 or RFC 2409).	All	T=O	
MA-CR-10	All Outer and Inner VPN Components shall use Cipher Block Chaining for IKE encryption.	All	T=O	
MA-CR-11	All Outer and Inner VPN Components shall use Cipher Block Chaining for ESP encryption with an HMAC for integrity.	All	T	MA-CR-12



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-CR-12	All Outer and Inner VPN Components shall use Galois Counter Mode for ESP encryption.	All	O	MA-CR-11
MA-CR-13	All Outer and Inner VPN Components shall set the IKE SA lifetime to at most 24 hours.	All	T=O	
MA-CR-14	All Outer and Inner VPN Components shall set the ESP SA lifetime to at most 8 hours.	All	T=O	
MA-CR-15	All VPN Components shall re-authenticate the identity of the VPN Component at the other end of the established tunnel before rekeying the IKE SA.	All	T=O	

12.4 INNER VPN COMPONENTS

Table 13. Inner VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-IR-1	The Inner VPN Component shall use Tunnel Mode IPsec or Transport Mode IPsec using an associated IP tunneling protocol (e.g. Transport Mode IPsec with GRE).	VI	T=O	
MA-IR-2	The packet size for packets leaving the external interface of the Inner VPN Component shall be configured to reduce packet fragmentation and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4) or Path MTU (PMTU) (for IPv6) and should consider Black network and Outer VPN Component MTU/PMTU values to achieve this.	VI	O	Optional
MA-IR-3	The Inner VPN Gateway shall not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network.	V	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-IR-4	The Inner VPN Client of EUDs shall encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g., DHCP) and locate the Inner VPN Gateway (i.e., DNS lookup of the VPN Component's IP address), in accordance with this CP.	VE	T=O	
MA-IR-5	The Inner VPN Component shall not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	V	T=O	

12.5 OUTER VPN COMPONENTS

Table 14. Outer VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-OR-1	Outer VPN Components shall use Tunnel Mode IPsec.	All	T=O	
MA-OR-2	Outer VPN Components shall not permit split-tunneling.	All	T=O	
MA-OR-3	The Outer VPN Component shall not allow any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.	All	T=O	
MA-OR-4	All traffic received by the Outer VPN Component on an interface connected to a Gray network, with the exception of Control Plane traffic not prohibited in the CP, shall have already been encrypted once.	All	T=O	
MA-OR-5	The Outer VPN Client of EUDs shall encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g. DHCP) in accordance with this CP (see Section 4.1.4).	VE, TE	T=O	
MA-OR-6	If one or more virtual machines are used to separate Outer and Inner VPN Clients on an EUD then the Outer VPN Client shall not run on the host operating system.	VE, TE	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-OR-7	Outer VPN Component shall not allow any packets received on an interface connected to a Black network to bypass decryption.	All	T=O	
MA-OR-8	Withdrawn			
MA-OR-9	Outer VPN Gateways shall not perform routing.	VI, TI	T=O	
MA-OR-10	If a Dedicated Outer VPN is utilized it shall be dedicated to a single security level and only provide the outer layer of IPsec to computing devices connecting to a Red network of the same security level.	VI, TI	T=O	

12.6 MULTIPLE SECURITY LEVEL REQUIREMENTS

The following section provides requirements for customers utilizing the same Outer VPN Gateway for multiple security levels as described in Section 4.2.4.

Table 15. Multiple Security Level Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MS-1	The solution shall include an Authentication Server in the Gray Management Network.	MS	T=O	
MA-MS-2	A unique device certificate shall be loaded on the Authentication Server along with the corresponding CA (signing) certificate.	MS	T=O	
MA-MS-3	The EUD shall establish a TLS session with the Outer VPN Gateway to exchange credentials.	MS	T=O	
MA-MS-4	The Outer VPN Gateway shall act as an EAP pass-through and forward authentication packet between the EUD and Authentication Server.	MS	T=O	
MA-MS-5	Upon successful authentication the Authentication Server shall send an Access Accept Radius packet to the Outer VPN Gateway including an attribute for which network the EUD is associated.	MS	T=O	
MA-MS-6	The Outer VPN Gateway shall utilize unique physical internal interfaces for each enclave of the solution (e.g., VLAN trunking of multiple enclaves is not permitted).	MS	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MS-7	The Outer VPN Gateway shall route EUD traffic over the appropriate interface and network based on the attribute provided by the Authentication Server in the Access Accept RADIUS packet.	MS	T=O	
MA-MS-8	The Outer VPN Gateway shall assign a firewall ACL to EUDs based on the attribute information provided by the Authentication Server.	MS	T=O	
MA-MS-9	The EUD and Outer VPN Gateway shall utilize TLS 1.2.	MS	T=O	
MA-MS-10	The EUD and Authentication Server shall use X.509 device certificates for mutual authentication.	MS	T=O	
MA-MS-11	The EUD and Outer VPN Gateway shall only use ciphers suites selected from the "TLS Cipher Suite (Threshold)" row of Table 9.	MS	T	MA-MS-12
MA-MS-12	TLS Components shall only use cipher suites selected from the "TLS Cipher Suite (Objective)" row of Table 9.	MS	O	MA-MS-11
MA-MS-13	Gray network components shall be physically protected to the level of the highest classified network.	MS	T=O	

12.7 TLS-PROTECTED SERVER & SRTP ENDPOINT REQUIREMENTS

Table 16. TLS-Protected Server & SRTP Endpoint Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-TE-1	TLS Components shall utilize TLS 1.2 or later.	T	T=O	
MA-TE-2	TLS Solution Infrastructure components shall terminate the Inner layer of encryption originating from TLS EUDs.	TI	T=O	
MA-TE-3	TLS Solution Infrastructure components shall use X.509 device certificates for mutual authentication with TLS EUDs.	TI	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-TE-4	Default, self-signed, or proprietary certificates, which are frequently preinstalled by the vendor, for the TLS Component shall be disabled.	T	T	MA-TE-5
MA-TE-5	Default, self-signed, or proprietary certificates, which are frequently preinstalled by the vendor, for the TLS Component shall be removed.	T	O	MA-TE-4
MA-TE-6	Unique device certificates shall be loaded onto TLS Components along with the corresponding Trust Anchor (signing) certificates.	T	T=O	
MA-TE-7	TLS Components shall only use ciphers suites selected from the "TLS Cipher Suite (Threshold)" row of Table 9.	T	T	MA-TE-8
MA-TE-8	TLS Components shall only use cipher suites selected from the "TLS Cipher Suite (Objective)" row of Table 9.	T	O	MA-TE-7



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative													
MA-TE-9	<p>SRTP Components shall only use algorithms selected from Table 10. Approved Commercial Algorithms for a Dedicated Outer VPN with Wireless Connectivity</p> <table border="1"> <thead> <tr> <th>Security Service</th> <th>Algorithm Suite</th> <th>Specifications</th> </tr> </thead> <tbody> <tr> <td rowspan="2">Confidentiality (Encryption)</td> <td>AES-128-CCMP (Threshold)</td> <td>FIPS PUB 197 IETF RFC 6239</td> </tr> <tr> <td>AES-256-GCMP (Objective)</td> <td>IETF RFC 6379 IETF RFC 6380 IETF RFC 6460</td> </tr> <tr> <td rowspan="2">EAP-TLS Cipher Suite</td> <td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold)</td> <td>IETF RFC 5216</td> </tr> <tr> <td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)</td> <td>IETF RFC 5246</td> </tr> </tbody> </table> <p>Table 11 that are approved to protect the highest classification level of the Red network data.</p>	Security Service	Algorithm Suite	Specifications	Confidentiality (Encryption)	AES-128-CCMP (Threshold)	FIPS PUB 197 IETF RFC 6239	AES-256-GCMP (Objective)	IETF RFC 6379 IETF RFC 6380 IETF RFC 6460	EAP-TLS Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold)	IETF RFC 5216	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)	IETF RFC 5246	T	T=O	
Security Service	Algorithm Suite	Specifications															
Confidentiality (Encryption)	AES-128-CCMP (Threshold)	FIPS PUB 197 IETF RFC 6239															
	AES-256-GCMP (Objective)	IETF RFC 6379 IETF RFC 6380 IETF RFC 6460															
EAP-TLS Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold)	IETF RFC 5216															
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)	IETF RFC 5246															
MA-TE-10	TLS Solution Infrastructure components shall not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	TI	T=O														

12.8 RETRANSMISSION DEVICE REQUIREMENTS

Table 17. Requirements for Retransmission Device



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RD-1	An EUD shall only connect to Retransmission Devices (RDs) authorized by a Government AO.	VE, TE	T=O	
MA-RD-2	An RD shall provide EUDs with connectivity to the Mobile Access Solution infrastructure via any Black Network using Wi-Fi or an Ethernet cable.	VE, TE	T=O	
MA-RD-3	If the RD is configured to be a Wi-Fi access point, the Wi-Fi network shall implement WPA2 AES-CCMP PSK or WPA2-Enterprise with a TLS-based EAP method.	VE, TE	T=O	
MA-RD-4	A RD shall not be utilized to protect Gray data between an Outer VPN Gateway and EUD.	VE, TE	T=O	
MA-RD-5	If the RD is configured to be a Wi-Fi access point using PSK, then the PSK shall use a length of at least 32 hexadecimal characters (or its equivalent).	VE, TE	T	MA-EU-26
MA-RD-6	RD shall only permit connections to devices on a Media Access Control (MAC) white list.	VE, TE	O	Optional
MA-RD-7	If the RD is configured as a Wi-Fi access point, then the PSK shall not be displayed on the RD.	VE, TE	T=O	
MA-RD-8	If the RD is configured as a Wi-Fi access point, then the Service Set Identification (SSID) shall not be displayed on the RD.	VE, TE	T=O	
MA-RD-9	If the RD is configured as a Wi-Fi access point, then the MAC address of connected devices shall not be displayed on the RD.	VE, TE	T=O	
MA-RD-10	The Administrator password shall not be displayed on the RD.	VE, TE	T=O	
MA-RD-11	The RD shall display the number of currently connected devices.	VE, TE	O	Optional
MA-RD-12	If the RD is configured to be a Wi-Fi access point, then Wi-Fi Protected Setup (WPS) shall be disabled.	VE, TE	T=O	
MA-RD-13	The RD shall be administered using HTTPS.	VE, TE	T=O	
MA-RD-14	The RD shall require authentication with Administrator credentials to make changes to RD settings.	VE, TE	T=O	
MA-RD-15	The RD default Administrator credentials shall be changed during provisioning.	VE, TE	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RD-16	The RD shall be configured to limit the number of connected devices to the maximum required for the mission.	VE, TE	T=O	
MA-RD-17	If the RD is configured as a Wi-Fi access point, then traffic of multiple EUDs sharing the RD shall be separated (commonly referred to as Wi-Fi Privacy Separation or AP Isolation).	VE, TE	T=O	
MA-RD-18	If the RD is configured as a Wi-Fi access point, then the RD shall disable broadcasting of the SSID.	VE, TE	O	Optional
MA-RD-19	The RD shall only permit charging on USB ports and interfaces.	VE, TE	O	Optional
MA-RD-20	The RD shall not permit connected EUDs to access files stored on the RD.	VE, TE	T=O	
MA-RD-21	The RD shall require Administrator authentication prior to downloading logs or configuration files.	VE, TE	T=O	
MA-RD-22	The RD shall only allow firmware updates signed by the RD manufacturer.	VE, TE	O	Optional
MA-RD-23	The RD shall prevent the ability to boot into recovery mode.	VE, TE	O	Optional
MA-RD-24	The RD shall require user or Administrator authentication prior to updating firmware.	VE, TE	O	Optional
MA-RD-25	If the RD is configured to be a Wi-Fi access point, the PSK shall use a length of at least 64 hexadecimal characters (or its equivalent).	VE, TE	O	MA-RD-5
MA-RD-26	If the RD is configured to be a Wi-Fi access point using WPA Enterprise, the certificate used for authentication shall be different from the certificates utilized to authenticate the outer and inner tunnels.	VE, TE	T=O	

12.9 WIRELESS CONNECTIVITY TO DEDICATED OUTER VPN

The following section provides requirements for EUDs utilizing a Dedicated Outer VPN connected to the computing device over wireless.



Mobile Access Capability Package



Table 18. Requirements for Wireless Connectivity to Dedicated Outer VPN

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-WC-1	A computing device shall only connect to a Dedicated Outer VPN authorized as part of the MA CP solution.	WC	T=O	
MA-WC-2	The Dedicated Outer VPN Wi-Fi network shall implement WPA2 AES-CCMP PSK or WPA2-Enterprise with a TLS-based EAP method.	WC	T=O	
MA-WC-3	If the Dedicated Outer VPN is configured using WPA2 PSK, then the PSK shall use a length of at least 32 hexadecimal characters (or its equivalent).	WC	T =O	
MA-WC-4	If the Dedicated Outer VPN is configured using WPA2 Enterprise, then the PSK shall use certificate based authentication.	WC	T =O	
MA-WC-5	If the Dedicated Outer VPN is configured using WPA2 Enterprise, then mutual authentication shall occur over the outer IPsec tunnel between the computing device and an Authentication Server in the Gray Management Network.	WC	T =O	
MA-WC-6	If the Dedicated Outer VPN is configured using WPA2 Enterprise, the computing device WLAN Client shall authenticate the identity of the Authentication Server by verifying that the Authentication Server's certificate chain is rooted by the outer trusted root Certificate Authority.	WC	T =O	
MA-WC-7	If the Dedicated Outer VPN is configured using WPA2 Enterprise, the computing device WLAN Client shall be configured to authenticate only specific servers through setting the client to accept only a Authentication Server certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	WC	T =O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-WC-8	If the Dedicated Outer VPN is configured using WPA2 Enterprise , a unique device certificate shall be loaded into the computing device WLAN Client along with the corresponding CA (signing) certificate.	WC	T=O	
MA-WC-9	The computing device WLAN Client shall negotiate new session keys with the Dedicated Outer VPN at least once per hour.	WC	T=O	
MA-WC-10	The computing device WLAN Client shall be prevented from using ad hoc mode (client-to-client connections).	WC	T=O	
MA-WC-11	The computing device WLAN Client shall be prevented from using network bridging.	WC	T=O	
MA-WC-12	The Dedicated Outer VPN shall only permit connections to computing devices on a MAC white list.	WC	T=O	
MA-WC-13	The Dedicated Outer VPN shall prohibit management by computing devices connected over wireless.	WC	T=O	
MA-WC-14	The Dedicated Outer VPN shall comply with all requirements in Table 12. Configuration Requirements for Inner and Outer VPN Components and Table 14. Outer VPN Components Requirements.	WC	T=O	

12.10 END USER DEVICES REQUIREMENTS

Table 19. Requirements for End User Devices

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-1	EUDs that do not implement an NSA-approved DAR solution and allow a user to store classified information on the EUD shall be treated as classified at all times. (See Section 4.2.1).	TE, VE	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-2	EUDs that implement an NSA-approved DAR solution (i.e., Data at Rest CP) shall comply with the handling requirements specified for the DAR solution.	VE, TE	T=O	
MA-EU-3	Withdrawn			
MA-EU-4	The Outer VPN Client private key store shall be separate from the private key store for the Inner VPN Client.	VE TE	T=O	
MA-EU-5	The Inner and Outer VPN Clients on the EUD shall be implemented on separate IP stacks. Implementations of IPv4 and IPv6 on the same operating system are considered to be part of the same IP stack.	VE	T=O	
MA-EU-6	If the EUD is not remotely administered, then it shall only be updated and rekeyed through re-provisioning.	VE, TE	T=O	
MA-EU-7	The EUD shall not allow split-tunneling.	VE, TE	T=O	
MA-EU-8	Rekeying of an EUD's certificates and associated private keys shall be done through re-provisioning prior to expiration of keys.	VE, TE	T	MA-EU-9
MA-EU-9	Rekeying of an EUD's certificates and associated private keys shall be done over the MA solution network prior to expiration of keys.	VE, TE	O	MA-EU-8
MA-EU-10	An EUD shall be de-authorized from the network and submitted for Forensic Analysis if suspected of being compromised.	VE, TE	T=O	
MA-EU-11	An EUD shall be destroyed if it has been determined to be compromised through Forensic Analysis.	VE, TE	T=O	
MA-EU-12	Users of EUDs shall successfully authenticate themselves to the services they access on the Red network using an AO-approved method.	VE, TE	T=O	
MA-EU-13	Red network services shall not transmit any classified data to EUDs until user authentication succeeds.	VE, TE	T=O	
MA-EU-14	Withdrawn			
MA-EU-15	All EUD Users shall sign an organization-defined user agreement before being authorized to use an EUD.	VE, TE	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-16	All EUD Users shall receive an organization-developed training course for operating an EUD prior to use.	VE, TE	T=O	
MA-EU-17	At a minimum, the organization-defined user agreement shall include each of the following: <ul style="list-style-type: none"> • Consent to monitoring • Operations Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when, where, and under what conditions the EUD may be used • Responsibility for reporting security incidents • Verification of IA Training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities 	VE, TE	T=O	
MA-EU-18	EUDs shall be dedicated for use solely in the MA solution, and not used to access any resources on networks other than the Red network it communicates with through the two layers of encryption.	VE, TE	T=O	
MA-EU-19	EUDs shall be remotely administered.	VE, TE	O	Optional
MA-EU-20	The EUD shall disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO.	VE, TE	T=O	
MA-EU-21	The EUD shall disable Firmware-Over-the-Air (FOTA) updates from the cellular carrier.	VE, TE	T=O	
MA-EU-22	The EUD shall disable all wireless interfaces (e.g. Bluetooth, NFC, Cellular, 802.11) that do not pass through the VPN client.	VE, TE	T=O	
MA-EU-23	The EUD shall disable processing of incoming cellular services including voice messaging services that do not pass through the VPN client.	VE, TE	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-24	All EUDs shall have their certificates revoked and resident image removed prior to disposal.	VE, TE	T=O	
MA-EU-25	Passwords for user to device (EUD selected from Mobile Platform section of CSfC Components List) authentication shall be a minimum of four alpha-numeric case sensitive characters.	VE, TE	T=O	
MA-EU-26	Withdrawn			
MA-EU-27	For a VPN EUD that has a VPN Gateway physically attached to it, the VPN Gateway shall be the outer layer of encryption and the VPN client on the EUD will be the Inner Layer of encryption.	VE	T=O	
MA-EU-28	Withdrawn			
MA-EU-29	If the EUD is using a physically attached Dedicated Outer VPN, the communication between the EUD and the Dedicated Outer VPN shall be through a wired connection (i.e., Ethernet) or Wi-Fi using WPA2.	VE, TE	T=O	
MA-EU-30	Withdrawn			
MA-EU-31	If the EUD is using a Dedicated Outer VPN to connect over the black transport network, the Dedicated Outer VPN shall be used to establish the outer layer of encryption.	VE, TE	T=O	
MA-EU-32	If an NSA-Approved DAR Solution is not implemented on EUDs, the native platform DAR protection shall be enabled.	VE, TE	T=O	
MA-EU-33	EUDs shall use a unique X.509 v3 device certificate, signed by the outer CA, for mutual authentication with Outer VPN Gateways.	VE, TE	T=O	
MA-EU-34	TLS EUDs shall either use a unique X.509 v3 device certificate, signed by the inner CA, or a unique X.509 v3 user certificate, signed by an authorized enterprise services CA, for mutual authentication with TLS-Protected Servers.	TE	T=O	
MA-EU-35	VPN EUDs shall use a unique X.509 v3 device certificate, signed by the inner CA, for mutual authentication with Inner VPN Gateways.	VE	T=O	
MA-EU-36	EUDs shall use an Access Point Name (APN) provided by a Domestic Cellular Carrier Private Network when utilizing Domestic Cellular Service as a Black Transport Network.	VE, TE	O	Optional



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-37	EUDs shall be configured for all IP traffic, with the exception of IKE, network address configuration, time synchronization, and name resolution traffic required to establish the IPsec tunnel, to flow through the IPsec VPN Client.	VE, TE	T	MA-EU-38
MA-EU-38	EUDs shall be configured for all IP traffic, with the exception of IKE, to flow through the IPsec VPN Client.	VE, TE	O	MA-EU-37
MA-EU-39	The EUD password lifetime shall be less than 181 days.	VE, TE	T=O	
MA-EU-40	The EUD screen shall lock after three minutes or less of inactivity.	VE, TE	T=O	
MA-EU-41	The EUD shall perform a wipe of all protected data after 10 or less authentication failures.	VE, TE	T=O	
MA-EU-42	VPN protection shall be enabled across the EUD.	VE, TE	T=O	
MA-EU-43	A security policy shall be configured on the EUD specific to each permitted Retransmission Device and/or Government Private Wireless network.	VE, TE	T=O	
MA-EU-44	During provisioning, all unnecessary keys shall be destroyed from the EUD secure key storage.	VE, TE	T=O	
MA-EU-45	During provisioning, all unnecessary X.509 certificates shall be removed from the EUD Trust Anchor Database.	VE, TE	T=O	
MA-EU-46	All display notifications shall be disabled while in a locked state.	VE, TE	O	Optional
MA-EU-47	USB mass storage mode shall be disabled on the EUDs.	VE, TE	T=O	
MA-EU-48	USB data transfer shall be disabled on the EUDs.	VE, TE	T=O	
MA-EU-49	Prior to updating the Application Processor system software, the system software digital signature shall be verified.	VE, TE	T=O	
MA-EU-50	Prior to installing new applications, the application digital signature shall be verified.	VE, TE	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-51	The EUD shall connect to the black network through a Government Private Wireless Network, Government Private Cellular Network, Domestic Cellular Network, Dedicated Outer VPN, or Retransmission device.	VE, TE	T=O	
MA-EU-52	If the EUD is using a physically attached Dedicated Outer VPN or retransmission device, the computing device shall not utilize Ethernet over USB.	VE, TE	T=O	
MA-EU-53	If EUDs utilize Government Private Wireless Networks for black transport, the Government Private Wireless Network shall be accredited by a Government AO.	VE, TE	T=O	
MA-EU-54	Application Restrictions – The end user shall only be able to access the applications that are necessary for the EUDs intended purpose.	VE, TE	T=O	
MA-EU-55	The end user shall not be able to change security relevant settings on the EUD.	VE, TE	T=O	
MA-EU-56	The EUD shall not be able to directly access the Black transport network. All traffic shall pass through the outer VPN tunnel.	VE, TE	T=O	
MA-EU-57	USB debugging capabilities shall be disabled on the EUDs.	VE, TE	T=O	
MA-EU-58	All EUDs shall display a consent prompt that requires users to accept prior to utilizing the device.	VE, TE	O	Optional

12.11 PORT FILTERING REQUIREMENTS FOR SOLUTION COMPONENTS

Table 20. Port Filtering Requirements for Solution Components

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PF-1	All components within the solution shall have all network interfaces restricted to the smallest address ranges, ports, and protocols possible.	All	T=O	
MA-PF-2	All Components within the solution shall have all unused network interfaces disabled.	All	T=O	
MA-PF-3	CDPs shall only allow inbound HTTP traffic.	C	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PF-4	For the Outer VPN Gateway interface connected to a Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	All	T=O	
MA-PF-5	For the Inner VPN Gateway interface connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and management and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	V	T=O	
MA-PF-6	The inner firewall shall implement an ACL which only permits ingress/egress traffic from/to Inner Encryption Endpoints.	All	T=O	
MA-PF-7	Any service or feature that allows an Outer VPN Gateway or an EUD to contact a third party server (such as one maintained by the manufacturer) shall be blocked.	All	T	MA-PF-8
MA-PF-8	Any service or feature that allows an Outer VPN Gateway or an EUD to contact a third party server (such as one maintained by the manufacturer) shall be disabled.	All	O	MA-PF-7
MA-PF-9	Multicast messages received on any interfaces of the Outer VPN Gateway, Gray Firewall, and inner encryption components shall be dropped.	All	T=O	
MA-PF-10	For solutions using IPv4, the Outer VPN Gateway shall drop all packets that use IP options.	All	O	Optional
MA-PF-11	For solutions using IPv4, the Outer VPN Gateway shall only accept packets with Transmission Control Protocol (TCP), User Data Protocol (UDP), ESP, or ICMP in the IPv4 Protocol field and drop all other packets.	All	T=O	
MA-PF-12	For solutions using IPv6, the Outer VPN Gateway shall only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PF-13	For all outer firewall interfaces, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	VI, TI	T=O	
MA-PF-14	EUDs consisting of a computing device shall prohibit ingress and egress of Certificate Revocation traffic (e.g. OCSP queries, HTTP GET to CDPs) on the Black interface.	VE, TE	T=O	
MA-PF-15	EUDs consisting of a single computing platform shall prohibit ingress and egress of Name Resolution traffic (e.g. DNS query/response) on the Black Interface.	VE, TE	O	Optional
MA-PF-16	EUDs consisting of a single computing platform shall prohibit ingress and egress of Network Time Protocol (NTP) traffic on the Black Interface.	VE, TE	O	Optional
MA-PF-17	For all outer firewall interfaces, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, EAP-TLS and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	VI, TI	T=O	MA-PF-13
MA-PF-18	Management plane traffic shall only be initiated from the Gray administrative work stations with the exception of logging or authentication traffic which may be initiated from outer VPN components.			
MA-PF-19	The Gray firewall shall only permit EUDs traffic to the Inner Encryption Component associated with the appropriate classification level.		T=O	

12.12 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 21. Configuration Change Detection Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-CM-1	A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-CM-2	An automated process shall ensure that configuration changes are logged.	All	T=O	
MA-CM-3	All solution components shall be configured with a monitoring service that detects all changes to configuration.	All	O	Optional

12.13 DEVICE MANAGEMENT REQUIREMENTS

Only authorized Security Administrators will be allowed to administer the components. The MA solution will be used as transport for the Secure Shell (SSH)v2, IPsec, or TLS data from the administration workstation to the component.

Table 22. Requirements for Device Management

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-DM-1	Administration workstations shall be dedicated for the purposes given in the CP and shall be physically separated from workstations used to manage non-CSfC solutions.	VI, TI	T=O	
MA-DM-2	The Inner Encryption Endpoints shall be managed from the Red network and the Outer VPN Gateway and Gray firewall shall be managed from the Gray network.	VI, TI	T=O	
MA-DM-3	A separate LAN or VLAN on the Red network shall be used exclusively for all management of Inner Encryption Endpoints and solution components within the Red network.	VI, TI	T=O	
MA-DM-4	A separate LAN or VLAN on the Gray network shall be used exclusively for all management of the Outer VPN Gateway, Gray firewall, and solution components within the Gray network.	VI, TI	T=O	
MA-DM-5	The Gray Management network shall not be directly connected to Non-Secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	VI, TI	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-DM-6	All administration of solution components shall be performed from an administration workstation remotely using NSA approved Capability Package or by managing the solution components locally.	VI, TI	T=O	
MA-DM-7	Security Administrators shall authenticate to solution components before performing administrative functions.	All	T	MA-DM-8
MA-DM-8	Security Administrators shall authenticate to solution components with Suite B-compliant certificates before performing administrative functions remotely.	All	O	MA-DM-7
MA-DM-9	Security Administrators shall establish a security policy for EUDs per the implementing organization's local policy.	VE, TE	T=O	
MA-DM-10	EUDs shall generate logs and send to a central SIEM in the Red network.	VE, TE	O	Optional
MA-DM-11	Security Administrators shall initiate certificate signing requests for solution components as part of their initial keying within the solution.	All	T=O	
MA-DM-12	Devices shall use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	All	O	Optional
MA-DM-13	The same administration workstation shall not be used to manage Inner Encryption Components and the Outer VPN Gateway.	VI, TI	T=O	
MA-DM-14	The Outer VPN Gateway and solution components within the Gray network shall forward log entries to a SIEM on the Gray Management network (or SIEM in the Red Network if using a CDS) within 10 minutes.	VI, TI	T=O	
MA-DM-15	Inner Encryption Components and solution components within the Red network shall forward log entries to a SIEM on the Red Management network within 10 minutes.	VI, TI	O	Optional
MA-DM-16	All logs forwarded to a SIEM on the Gray Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	All	O	Optional
MA-DM-17	All logs forwarded to a SIEM on a Red Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	All	O	Optional
MA-DM-18	Withdrawn			



Mobile Access Capability Package



12.14 CONTINUOUS MONITORING REQUIREMENTS

Table 23. Continuous Monitoring Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MR-1	Traffic from the Black, Gray, or Red networks shall be monitored from an Intrusion Detection System (IDS).	VI, TI	T	MA-MR-2
MA-MR-2	Traffic from the Black, Gray, or Red networks shall be monitored from an Intrusion Prevention System (IPS).	VI, TI	O	MA-MR-1
MA-MR-3	An IDS shall be deployed between the outer VPN and Gray firewall (M2) and inside the inner firewall (M3).	VI, TI	T	MA-MR-4 MA-MR-5 MA-MR-6
MA-MR-4	An IDS shall be deployed between the outer firewall and Outer VPN (M1), and between the Outer VPN and Gray firewall (M2), and inside the inner firewall (M3), and between the Gray firewall and Inner encryption gateway (M4).	VI, TI	O	MA-MR-3 MA-MR-5 MA-MR-6
MA-MR-5	An IPS shall be deployed between the Outer VPN and Gray firewall (M2) and inside the Inner firewall (M3).	VI, TI	O	MA-MR-3 MA-MR-4 MA-MR-6
MA-MR-6	An IPS shall be deployed between the Outer firewall and Outer VPN (M1), and between the Outer VPN and Gray firewall (M2), and inside the Inner firewall (M3), and between the Gray firewall and Inner encryption gateway (M4).	VI, TI	O	MA-MR-3 MA-MR-4 MA-MR-5
MA-MR-7	Each IDS in the solution shall be configured to provide a dashboard or send alerts to the Security Administrator.	VI, TI	T	MA-MR-8
MA-MR-8	Each IPS in the solution shall be configured to block malicious traffic flows and alert the Security Administrator.	VI, TI	O	MA-MR-7
MA-MR-9	Each IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	VI, TI	T	MA-MR-10
MA-MR-10	Each IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	VI, TI	O	MA-MR-9
MA-MR-11	Each IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	VI, TI	T	MA-MR-12



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MR-12	Each IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	VI, TI	O	MA-MR-11
MA-MR-13	A SIEM component shall be placed within the Gray network unless devices are configured to push events to a Red network SIEM through an approved CDS.	VI, TI	T=O	
MA-MR-14	The SIEM shall be configured to send alerts to the Security Administrator when anomalous behavior is detected (i.e. blocked packets from the Outer VPN Gateway or Gray firewall).	VI, TI	T=O	
MA-MR-15	The Gray SIEM shall collect logs from the Outer VPN Gateway, Gray firewall, and any components located within the Gray Management Services.	VI, TI	T=O	
MA-MR-16	Logs sent to the Gray SIEM shall be encrypted with TLS.	VI, TI	O	
MA-MR-17	The Gray SIEM shall maintain an up to date table of Certificate Common Name and assigned IP address utilized for the Outer IPsec tunnel.	All	T=O	
MA-MR-18	The Gray SIEM shall provide a dashboard or alert for EUDs attempting to establish a connection with the Outer VPN Gateway utilizing misconfigured VPN Client settings.	All	T=O	
MA-MR-19	The Gray SIEM shall provide a dashboard or alert for three or more invalid login attempts in a 24 hour period to the Outer VPN Gateway or Gray firewall.	All	T=O	
MA-MR-20	The Gray SIEM shall maintain a listing of privilege escalations on the Outer VPN Gateway and Gray firewall.	All	T=O	
MA-MR-21	The Gray SIEM shall provide an alert or dashboard of configuration changes to the Outer VPN Gateway and Gray firewall	All	T=O	
MA-MR-22	The Gray SIEM shall provide an alert or dashboard of new accounts created on the Outer VPN Gateway, Gray firewall, and any Gray Authentication Server.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MR-23	The Gray SIEM shall provide an alert or dashboard for attempted IPsec connections to the Outer VPN Gateway which utilized an invalid certificate.	All	T=O	
MA-MR-24	The Gray SIEM shall provide a graph or table of blocked traffic at the Gray firewall grouped by EUD Common Name.	All	T=O	
MA-MR-25	The Gray SIEM shall maintain a dashboard of DNS queries outside of expected values for IP addresses and domains.	All	O	Optional
MA-MR-26	Network flow data shall be enabled on all routers and switches in the Red network.	All	T=O	
MA-MR-27	A network flow data collector (e.g., SiLK, IPFlow, NetFlow Collector) shall be installed in the Red network.	All	T=O	
MA-MR-28	A baseline for network flow data shall be established.	All	O	Optional
MA-MR-29	A baseline for network flow data shall be updated regularly.	All	O	Optional
MA-MR-30	Network flow data shall be reviewed daily for: <ul style="list-style-type: none"> Systems generating excessive amounts of traffic Systems trying to connect to improper IP addresses Systems trying to connect to closed ports on internal servers 	All	O	Optional
MA-MR-31	Network flow data shall be reviewed for systems generating excessive number of short packets (over 60% of packets containing 150 or less bytes).	All	O	Optional
MA-MR-32	Network flow data shall be reviewed for excessive numbers of ICMP messages.	All	O	Optional

12.15 AUDITING REQUIREMENTS

Table 24. Auditing Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-1	VPN Gateways shall log establishment of a VPN tunnel.	T, V	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-2	TLS-Protected Servers shall log establishment of a TLS connection.	TI	T=O	
MA-AU-3	VPN Gateways shall log termination of a VPN tunnel.	T, V	T=O	
MA-AU-4	TLS-Protected Servers shall log termination of a TLS connection.	TI	T=O	
MA-AU-5	VPN Clients shall log establishment of a VPN tunnel.	VE, TE	O	Optional
MA-AU-6	TLS Clients shall log establishment of a TLS tunnel	TE	O	Optional
MA-AU-7	VPN Clients shall log termination of a VPN tunnel.	VE, TE	O	Optional
MA-AU-8	TLS Client shall log termination of a TLS tunnel.	TE	O	Optional
MA-AU-9	Solution components shall log all actions performed on the audit log (off-loading, deletion, etc.).	VI, TI	T=O	
MA-AU-10	Solution components shall log all actions involving identification and authentication.	VI, TI	T=O	
MA-AU-11	Solution components shall log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.	TI,VI	T=O	
MA-AU-12	Solution components shall log all actions performed by a user with super-user or administrator privileges.	VI, TI	T=O	
MA-AU-13	Solution components shall log escalation of user privileges.	VI, TI	T=O	
MA-AU-14	Solution components shall log generation, loading, and revocation of certificates.	All	T=O	
MA-AU-15	Solution components shall log changes to time.	VI, TI	T=O	
MA-AU-16	Each log entry shall record the date and time of the event.	All	T=O	
MA-AU-17	Each log entry shall include the identifier of the event.	All	T=O	
MA-AU-18	Each log entry shall record the type of event.	All	T=O	
MA-AU-19	Each log entry shall record the success or failure of the event to include failure code, when available.	All	T=O	
MA-AU-20	Each log entry shall record the subject identity.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-21	Each log entry shall record the source address for network-based events.	All	T=O	
MA-AU-22	Each log entry shall record the user and, for role-based events, role identity, where applicable.	All	T=O	
MA-AU-23	Auditors shall detect when two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	V	O	Optional
MA-AU-24	Auditors shall detect when two or more simultaneous TLS connections from different IP addresses are established using the same EUD device certificate.	T	O	Optional
MA-AU-25	Upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated CRL to the Security Administrator.	V	O	Optional
MA-AU-26	Upon notification of two or more simultaneous TLS connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated CRL to the Security Administrator.	T	O	Optional
MA-AU-27	The Security Administrator shall immediately drop the session upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate.	V	O	Optional
MA-AU-28	The Security Administrator shall immediately drop the session upon notification of two or more simultaneous TLS connections from different IP addresses using the same EUD device certificate.	T	O	Optional
MA-AU-29	VPN Gateways shall log the failure to download a CRL from a CDP.	VI	T=O	
MA-AU-30	TLS-Protected Servers shall log the failure to download a CRL from a CDP.	TI	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-31	VPN Gateways shall log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	VI	T=O	
MA-AU-32	TLS-Protected Servers shall log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	TI	T=O	
MA-AU-33	VPN Gateways shall log if signature validation of the CRL downloaded from a CDP fails.	VI	T=O	
MA-AU-34	TLS-Protected Servers shall log if signature validation of the CRL downloaded from a CDP fails.	TI	T=O	
MA-AU-35	Auditors shall compare and analyze collected network flow data against the established baseline on at least a weekly basis.	VI, TI	O	Optional
MA-AU-36	Locally-run CAs shall comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	VI, TI	T=O	
MA-AU-37	Locally-run CAs shall comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	VI, TI	T=O	
MA-AU-38	Audits and assessments for outer and inner CAs shall be performed by personnel who are knowledgeable in the CAs' operations, as well as the CAs' CP and CPS requirements and processes, respectively.	VI, TI	T=O	

12.16 KEY MANAGEMENT REQUIREMENTS

12.16.1 GENERAL REQUIREMENTS

Table 25. PKI General Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-1	User certificates and user private keys shall be classified to the level determined by the AO.	TE, VE	T=O	
MA-KM-2	Outer CAs shall provide services through either the Gray or Red network.	VI, TI	T = O	
MA-KM-3	Inner CAs shall provide services through the Red network.	VI, TI	T=O	
MA-KM-4	Locally run inner tunnel CAs shall be physically separate from locally-run outer tunnel CAs.	VI, TI	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-5	All certificates issued by the outer and inner CAs for the MA Solution shall be Non-Person Entity (NPE) certificates, except in the one case when a TLS EUD requires a user certificate for the inner TLS tunnel.	VI, TI	T=O	
MA-KM-6	All certificates issued by the outer and inner CAs for the MA solution shall be used for authentication only.	VI, TI	T=O	
MA-KM-7	Authentication certificates issued by the outer and inner CAs for the MA solution shall be X.509 v3 certificates as defined in ITU-T Recommendation X.509.	VI, TI	T=O	
MA-KM-8	Authentication certificate profiles for the outer and inner CAs for the MA solution shall comply with IETF RFC 5280.	VI, TI	T=O	
MA-KM-9	All device certificates issued by the outer and inner CAs, and their corresponding private keys, shall be treated as CUI (or higher as determined by the AO).	All	T=O	
MA-KM-10	The key sizes and algorithms for CA certificates and authentication certificates issued to Outer VPN Components, Inner Encryption Components, and Administrative Device Components shall be as specified in CNSS Advisory Memorandum 02-15 or subsequent revisions to CNSSP 15 (See Table 8)	All	T=O	
MA-KM-11	Outer and inner CAs shall not have access to private keys used in the MA Solution Components.	All	T=O	
MA-KM-12	Private keys associated with on-line, locally run outer and inner CAs shall be protected using Hardware Security Modules (HSMs) validated to at least FIPS 140-2 Level 2. "On-line" means the CA is always powered on and network-accessible.	VI, TI	T=O	
MA-KM-13	Outer and inner CAs shall operate in compliance with a Certificate Policy and Certification Practices Statement that is formatted in accordance with IETF RFC 3647.	VI, TI	T=O	



Mobile Access Capability Package



12.16.2 CERTIFICATE ISSUANCE REQUIREMENTS

Table 26. Certificate Issuance Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-14	Outer VPN Components, Inner Encryption Components, and Gray and Red Management Services Components shall be initially keyed and loaded with certificates within a physical environment certified to protect the highest classification level of the MA solution network.	All	T=O	
MA-KM-15	Private keys for Outer VPN Components, Inner Encryption Components and Gray and Red Management Services Components shall never be escrowed.	All	T=O	
MA-KM-16	Outer and inner CAs shall use Public Key Cryptographic Standard (PKCS) #10 and PKCS#7 to issue authentication certificates to Outer VPN Components, Inner Encryption Components, and Gray and Red Management Services components.	VI, TI	T	MA-KM-19
MA-KM-17	Red and Gray Management Services shall use PKCS#12 for installing certificates/keys to EUDs.	All	T	MA-KM-18
MA-KM-18	Red and Gray Management Services shall use PKCS#7 for installing certificates to EUDs.	All	O	MA-KM-17
MA-KM-19	Outer and inner CAs shall use IETF RFC 7030 EST to issue authentication certificates to Outer VPN Components, Inner Encryption Components, and Gray and Red Management Services Components.	All	O	MA-KM-16
MA-KM-20	Certificate requests for Outer VPN Components, Inner Encryption Components and Gray and Red Management Services Components shall be submitted to the CA in accordance with the CA's Certificate Policy and Certification Practices Statement (CPS).	All	T=O	
MA-KM-21	Outer and inner CAs shall issue certificates in accordance with their Certificate Policies and CPSs.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-22	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure the CAs issue certificates within a defined and limited name space and assert: <ul style="list-style-type: none"> • Unique Distinguished Names (DN) • Appropriate key usages • A registered policy OID 	All	T=O	
MA-KM-23	Inner and outer CAs shall assert at least one CRL CDP Uniform Resource Locator (URL) in certificates issued to Solution Infrastructure Outer VPN Gateways, Inner Encryption Components, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRLs.	All	T=O	
MA-KM-24	The key validity period for certificates issued by non-Enterprise, locally run CAs to MA End User Devices shall not exceed 14 months.	All	T=O	
MA-KM-25	The key validity period for certificates issued by non-Enterprise, locally run CAs to MA Solution Infrastructure Components shall not exceed 36 months.	All	T=O	
MA-KM-26	Inner CAs shall only issue certificates to Inner Encryption Components and Red Network Components of MA Solutions.	All	T=O	
MA-KM-27	Outer CAs shall only issue certificates to Outer VPN Components and Gray Network Components of MA Solutions.	All	T=O	
MA-KM-28	Withdrawn			
MA-KM-29	Withdrawn			
MA-KM-30	Certificates issued to Outer VPN Gateways must assert the IP address of the Outer VPN gateway in either the Common Name field of the Distinguished Name, or the Subject Alternative Name certificate extension.	VI	O	
MA-KM-31	Over-the-network renewal and rekey of authentication certificates to EUDs shall be done using two valid MA CP encryption layers to the EUD in cases where EST is not supported.	All	O	



Mobile Access Capability Package



12.16.3 CERTIFICATE RENEWAL AND REKEY REQUIREMENTS

Table 27. Certificate Renewal and Rekey Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-31	Certificate renewal or rekey shall occur prior to a certificate expiring. If renewal/rekey occurs after a certificate expires, then the initial certificate issuance process is used to renew/rekey the certificate.	All	T=O	
MA-KM-32	Certificate renewal or rekey shall be performed in accordance with the CA's Certificate Policy and CPS.	All	T=O	
MA-KM-33	Inner and outer CAs shall issue renewed/rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7.	All	T	MA-KM-36
MA-KM-34	Withdrawn			
MA-KM-35	Withdrawn			
MA-KM-36	Inner and outer CAs shall support over-the-network renewal and rekey of authentication certificates to Solution Components using EST (IETF RFC 7030).	All	O	MA-KM-33

12.16.4 CERTIFICATE REVOCATION AND CDP REQUIREMENTS

Table 28. Requirements for Certificate Revocation and CDPs

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-37	Inner and outer CAs shall revoke a certificate issued to Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	VI, TI	T=O	
MA-KM-38	Inner and outer CAs shall make certificate revocation information available in the form of CRLs signed by the CAs.	VI, TI	T=O	
MA-KM-39	CRLs shall be X.509 v2 CRLs as defined in ITU-T Recommendation X.509.	C	T=O	
MA-KM-40	CRL profiles shall comply with IETF RFC 5280.	C	T=O	
MA-KM-41	Procedures for requesting certificate revocation shall comply with the CA's Certificate Policy and Certification Practices Statement.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-42	<p>Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure revocation procedures address the following:</p> <ul style="list-style-type: none"> • Response for a lost, stolen or compromised MA EUD • Removal of a revoked infrastructure device (i.e., VPN Gateway) from the network • Re-establishment of an MA Solution Component whose certificate was revoked • Revocation of certificates due to compromise of an MA EUD • Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP addresses 	All	T=O	
MA-KM-43	Inner and outer CAs shall make CRLs available to authorized CRL Distribution Points (CDPs), so that the CRLs can be accessed by Solution Components.	C	T=O	
MA-KM-44	Enterprise CAs shall create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	VI, TI	T=O	
MA-KM-45	Non-enterprise, locally run CAs shall publish new CRLs at least once every 28 days.	VI, TI	T=O	
MA-KM-46	Non-enterprise, locally run CAs shall create a new CRL within one hour of a certificate being revoked.	VI, TI	T=O	
MA-KM-47	Solution Infrastructure Components shall have access to new certificate revocation information within 24 hours of the CA creating a new CRL.	VI, TI	T=O	
MA-KM-48	Non-enterprise, locally run CAs shall ensure that newly created CRLs are published at least 7 days prior to the expiration of the current CRLs.	VI, TI	T=O	
MA-KM-49	The Solution shall provide certificate revocation status information via an Online Certificate Status Protocol (OCSP) Server on the Red and Gray network that is compliant with IETF RFC 6960.	VI, TI	O	Optional



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-50	Certificate revocation status messages delivered by an OCSP server shall be digitally signed and compliant with IETF RFC 6960.	VI, TI	O	Optional

12.16.5 PRE-SHARED KEY (PSK) REQUIREMENTS

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-51	PSKs used for WPA2 shall be 128 bits.	WC	T	
MA-KM-52	PSKs used for WPA2 shall be 256 bits.	WC	O	
MA-KM-53	PSKs shall be generated by NSA-approved devices.	WC	T=O	
MA-KM-54	PSKs shall be distributed to, and installed on CSfC devices in a manner that minimizes the exposure of the red PSK to the greatest extent possible.	WC	T=O	
MA-KM-55	Trusted personnel shall be used to generate, distribute and install PSKs onto CSfC devices.	WC	T=O	
MA-KM-56	PSKs shall be periodically updated based on the threat environment. The higher the threat environment, the more often the PSKs are to be updated.	WC	T=O	
MA-KM-57	A PSK shall be updated on all CSfC devices that utilize the PSK as soon as practically possible if the PSK is considered or suspected to be compromised.	WC	T=O	
MA-KM-58	If a PSK is considered or suspected to be compromised, a CSfC device utilizing that PSK shall not be used until the PSK is updated.	WC	T=O	

13 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

13.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.



Mobile Access Capability Package



Table 29. Requirements for the Use and Handling of Solutions

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-1	All Solution Infrastructure components shall be physically protected as classified devices, classified at the level of the Red network.	VI, TI	T=O	
MA-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the solution Infrastructure components.	VI, TI	T=O	
MA-GD-3	Only authorized and appropriately cleared users, administrators, and security personnel shall have physical access to EUDs when in a classified state.	VE, TE	T=O	
MA-GD-4	All components of the solution shall be disposed of as classified devices, unless declassified using AO-approved procedures.	All	T=O	
MA-GD-5	EUDs using an NSA-approved DAR solution shall be disposed of in accordance with the disposal requirements for the DAR solution.	VE, TE	T=O	
MA-GD-6	All EUDs shall have their certificates revoked prior to disposal.	VE, TE	T=O	
MA-GD-7	Users shall periodically inspect the physical attributes of EUDs for signs of tampering or other unauthorized changes.	VE, TE	T=O	
MA-GD-8	Acquisition and procurement documentation shall not include information concerning the purpose of the equipment.	All	T=O	
MA-GD-9	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the MA CP.	All	T=O	
MA-GD-10	The AO will ensure that a compliance audit shall be conducted every year against the latest version of the MA CP as part annual solution re-registration process.	All	T=O	
MA-GD-11	Results of the compliance audit shall be provided to, and reviewed by, the AO.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-12	Customers interested in registering their solution against the MA CP shall register with NSA and receive approval prior to AO authorization to operate.	All	T=O	
MA-GD-13	The implementing organization shall complete and submit an MA CP requirements compliance matrix to their respective AO.	All	T=O	
MA-GD-14	Registration and re-registration against the MA CP shall include submission of MA CP registration forms and compliance matrix to NSA.	All	T=O	
MA-GD-15	When a new approved version of the MA CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months.	All	T=O	
MA-GD-16	Solution implementation information, which was provided to NSA during solution registration, shall be updated annually (in accordance with Section 15.3) as part of an annual solution re-registration process.	All	T=O	
MA-GD-17	Audit log data shall be maintained for a minimum of 1 year.	All	T=O	
MA-GD-18	The amount of storage remaining for audit events shall be assessed by the security administrator quarterly in order to ensure that adequate memory space is available to continue recording new audit events.	All	T=O	
MA-GD-19	Audit data shall be frequently off-loaded to a backup storage medium.	All	T=O	
MA-GD-20	The implementing organization shall develop a set of procedures to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	All	T=O	
MA-GD-21	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-22	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long-term storage.	All	T=O	
MA-GD-23	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product.	All	T=O	
MA-GD-24	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	All	T=O	
MA-GD-25	Strong passwords shall be used that comply with the requirements of the AO.	VI, TI	T=O	
MA-GD-26	The implementing organization shall test and subsequently apply security critical patches to all components in the solution in accordance with local policy and this CP.	All	T=O	
MA-GD-27	Local policy shall dictate how the Security Administrator will install patches to solution components.	All	T=O	
MA-GD-28	Solution components shall comply with local TEMPEST policy.	All	T=O	
MA-GD-29	Software, settings, keys, and all other configuration data persistently stored on EUDs shall be handled as controlled unclassified information or higher classification.	All	T=O	
MA-GD-30	All hardware components shall be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC Solution.	All	T=O	

Additional MA-GD requirements can be found in Section 14.

13.2 REQUIREMENTS FOR INCIDENT REPORTING

Table 30 lists requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators, Certificate Authority



Mobile Access Capability Package



Administrators (CAAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

For the purposes of incident reporting, “malicious” activity includes not only events that have been attributed to activity by an adversary but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Table 30 only provides requirements directly related to the incident reporting process. See Section 12.14 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 30. Incident Reporting Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RP-1	Solution owners shall report confirmed incidents meeting the criteria in MA-RP-3 through MA-RP-16 within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	All	T=O	
MA-RP-2	At a minimum, the organization shall provide the following information when reporting security incidents: <ul style="list-style-type: none"> • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Name of affected Network(s) • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No) 	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RP-3	Solution owners shall report a security failure in any of the CSfC solution components.	All	T=O	
MA-RP-4	Solution owners shall report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC Solution.	All	T=O	
MA-RP-5	For all Gray network interfaces, solution owners shall report any malicious inbound and outbound traffic.	All	T=O	
MA-RP-6	Solution owners shall report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	All	T=O	
MA-RP-7	Solution owners shall report if a solution component sends traffic with an unauthorized destination address.	All	T=O	
MA-RP-8	Solution owners shall report any malicious configuration changes to the components.	All	T=O	
MA-RP-9	Solution owners shall report any unauthorized escalation of privileges to any of the CSfC solution components.	All	T=O	
MA-RP-10	Solution owners shall report if two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	All	T=O	
MA-RP-11	Solution owners shall report any evidence of malicious physical tampering with solution components.	All	T=O	
MA-RP-12	Solution owners shall report any evidence that one or both of the layers of the solution failed to protect the data.	All	T=O	
MA-RP-13	Solution owners shall report any significant degradation of services provided by the solution.	All	T=O	
MA-RP-14	Solution owners shall report malicious discrepancies in the number of VPN connections established by Outer VPN Gateways.	All	T=O	
MA-RP-15	Solution owners shall report malicious discrepancies in the number of VPN connections established by the Inner VPN Gateway	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RP-16	Solution owners shall report malicious discrepancies in the number of TLS connections established by the TLS-Protected Server	T	T=O	

14 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the MA solution. Security Administrator duties include but are not limited to the following:

- 1) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.
- 2) Documenting and reporting security-related incidents to the appropriate authorities.
- 3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.
- 4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the MA solution.
- 5) Ensuring that the implemented MA solution remains compliant with the latest version of this CP.
- 6) Provisioning and maintaining EUDs in accordance with this CP for implementations that include them.

Certificate Authority Administrator (CAA) – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to the following:

- 1) Administering the CA, including authentication of all components requesting certificates.
- 2) Maintaining and updating the CRL.
- 3) Provisioning and maintaining EUD certificates in accordance with this CP for implementations that include them.



Mobile Access Capability Package



Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the MA solution. Auditor duties include, but are not limited to, the following:

- 1) Reviewing, managing, controlling, and maintaining security audit log data.
- 2) Documenting and reporting security-related incidents to the appropriate authorities.
- 3) The Auditor will only be authorized access to Outer and Inner administrative components.

Integrator – In certain cases, an external Integrator may be hired to implement an MA solution based on this CP. Integrator duties may include, but are not limited to:

- 1) Acquiring the products that compose the solution.
- 2) Configuring the MA solution in accordance with this CP.
- 3) Documenting, testing, and maintaining the solution.
- 4) Responding to incidents affecting the solution.

End User –An End User may operate an EUD from physical locations not owned, operated, or controlled by the government. The End User shall be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. Remote User duties include, but are not limited to, the following:

- 1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.
- 2) Alerting the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

Additional policies related to the personnel that perform these roles in an MA Solution are as follows:

Table 31. Role-Based Personnel Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-31	The Security Administrator, CAAs, Auditor, EUD User, and Integrators shall be cleared to the highest level of data protected by the solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement.	All	T=O	



Mobile Access Capability Package



Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-32	The Security Administrator, CAA, and Auditor roles shall be performed by different people.	All	T=O	
MA-GD-33	All Security Administrators, CAAs, EUD Users, and Auditors shall meet local Information Assurance (IA) training requirements.	All	T=O	
MA-GD-34	The CAA(s) for the inner tunnel shall be different individuals from the CAA(s) for the Outer tunnel.	All	O	Optional
MA-GD-35	Upon discovering an EUD is lost or stolen, an EUD User shall immediately report the incident to their Security Administrator and Certificate Authority Administrator.	VE, TE	T=O	
MA-GD-36	Upon notification of a lost or stolen EUD, the Certificate Authority Administrators shall revoke that EUD's certificates.	VE, TE	T=O	
MA-GD-37	The Security Administrator(s) for the Inner Encryption Endpoints and supporting components on Red networks shall be different individuals from the Security Administrator(s) for the Outer VPN Gateway and supporting components on Gray networks.	All	T=O	
MA-GD-38	Administrators shall periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	All	O	Optional
MA-GD-39	The Auditor shall review all logs specified in this CP at least once a week.	All	T=O	
MA-GD-40	Security Administrators shall initiate the certificate revocation process prior to disposal of any solution component.	All	T=O	
MA-GD-41	Auditing of the outer and inner CA operations shall be performed by individuals who were not involved in the development of the CP and CPS, or integration the MA solution.	All	T=O	

15 INFORMATION TO SUPPORT THE AO

This section details items that likely will be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:



Mobile Access Capability Package



- The customer, possibly with support from an Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a test plan and perform testing of the MA solution, see Section 15.1.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 15.2.
- The customer provides the results from testing and system certification and accreditation to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented in accordance with the CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 15.3.
- Customers who want to use a variant of the solution detailed in this CP will contact their NSA/IAD Client Advocate to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit shall be conducted every year against the latest version of the MA CP, and the results shall be provided to the AO.
- The AO will ensure that certificate revocation information is updated on all the Solution Components in the solution in the case of a compromise.
- The AO will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.
- The AO will report incidents affecting the solution in accordance with Section 13.2.

The system AO maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO shall ensure that the solution remains properly configured with all required security updates implemented.

15.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of an MA solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the MA solution.



Mobile Access Capability Package



The entire solution, to include each component described in Section 5 and 5.8, is addressed by this test plan including the following:

- 1) Set up the baseline network and configure all components.
- 2) Document the baseline network configuration. Include product model and serial numbers, and software version numbers at a minimum.
- 3) Develop a test plan for the specific implementation using the test requirements from Section 16. Any additional requirements imposed by the local AO should also be tested, and the test plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.
- 4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black box testing and Gray box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
- 5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO for approval of the solution.

The following testing requirement has been developed to ensure that the MA solution functions properly and meets the configuration requirements from Section 12. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 32. Test Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-TR-1	The organization implementing the CP shall perform all tests listed in Section 16.	All	T=O	

15.2 RISK ASSESSMENT

The risk assessment of the MA solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.



Mobile Access Capability Package



15.3 REGISTRATION OF SOLUTIONS

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. This registration will allow NSA to track where MA CP solutions are instantiated and to provide the AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available at http://www.nsa.gov/ia/programs/csfc_program.

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this CP that has been approved by the IAD Director is published, customers will have six months to bring their solutions into compliance with the new version of the CP and re-register their solution (see requirement MA-GD-15). Customers are also required to update their registrations whenever the information provided on the registration form changes.

16 TESTING REQUIREMENTS

This section is being improved and re-written for MA CP Version 2.0.



Mobile Access Capability Package



APPENDIX A. GLOSSARY OF TERMS

Authorization (To Operate) – The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

Authorization Boundary – All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Authorizing Official – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorizing Official Designated Representative – An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

Authorization Package – A security package of documents consisting of the security control assessment that provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

Assurance – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit Log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective actions are required.

Availability – Ensuring timely and reliable access to and use of information. (NIST SP 800-37).

Black Box Testing – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).



Mobile Access Capability Package



Black Network – A network that contains classified data that has been encrypted twice. (See Section 4.1.3)

CP – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. CP instantiations are built using products selected from the CSfC Components List.

Central Management Site – A site within a MA solution that is responsible for remotely managing the solution components located at other sites (see Section 4.2.3).

Certificate Authority (CA) – An authority trusted by one or more users to create and assign certificates. (ISO9594-8)

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. (IETF RFC 3647)

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Computing Device – An EUD such as a phone, laptop, or tablet.

Confidentiality – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure, and confidence that only the appropriate set of individuals or organizations would be provided the information.

Control Plane Protocol – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

CRL Distribution Point (CDP) – A web server that hosts a copy of a CRL issued by a CA for VPN Components to download (see Section 9.1).

Cross Domain Solution (CDS) – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

Data Plane Protocol – A protocol that carries the data being transferred through the solution.

Dedicated Outer VPN - A dedicated piece of hardware that can be part of an EUD and terminates the outer layer of IPsec encryption.



Mobile Access Capability Package



End User Device (EUD) – A form-factor agnostic component of the Mobile Access solution that can include a mobile phone, tablet, or laptop computer. EUDs can be composed of multiple components to provide physical separation between layers of encryption (see Section 4.2.1 for explanation of detailed differences between VPN EUD and TLS EUD solution design options).

Enterprise/Red Network – A network that contains unencrypted classified data and can contain singly encrypted gray data (see Section 4.1.1).

External Interface – The interface of the Outer VPN Gateway that connects to the internal interface of the Outer firewall.

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Box Testing – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e. knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

Gray Network – A network that contains classified data that has been encrypted once (see Section 4.1.2).

Gray Firewall – A stateful traffic filtering firewall placed on the Gray network to provide filtering of ports, protocols, and IP addresses to ensure traffic reaches the correct Inner Encryption Endpoint or is dropped.

Internal Interface – The interface on a VPN Gateway or Inner Encryption Component that connects to the inner network (i.e., the Gray network on the Outer VPN Gateway or the Red network on the Inner Encryption Component).

Locally Managed Device – A device that is being managed by the direct connection of the Administration Workstation to the device in a hardwired fashion (such as a console cable).

Malicious – Any unauthorized events that are either unexplained or in any way indicate adversary activity.

Management Plane Protocol – A protocol that carries either traffic between a system administrator and a component being managed, or log messages from a solution component to a SIEM or similar repository.

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.



Mobile Access Capability Package



Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Remotely Managed Device – A device that is being managed by any other method besides that given in the definition of a Locally Managed Device.

Security Level – The combination of classification level, list of compartments, dissemination controls, and other controls applied to the information within a network.

Split-tunneling – Allows network traffic to egress through a path other than the established VPN tunnel (either on the same interface or another network interface). Split tunneling is explicitly prohibited in MA CP compliant configurations (see MA-OR-2 and MA-EU-7).

SRTP Client – A component on the EUD that facilitates encryption for voice communications.

TLS Client – A component on a TLS EUD that can provides the Inner layer of DIT encryption.

TLS Component – Refers to both TLS Clients and TLS-Protected Servers.

VPN Client – A VPN application installed on an EUD.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – A VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in a secure facility and includes Inner and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include EUDs.

APPENDIX B. ACRONYMS

Acronym	Definition
AES	Advanced Encryption Standard
AO	Authorizing Official
APN	Access Point Name
ARP	Address Resolution Protocol
BIOS	Basic Input/Output System
BGP	Border Gateway Protocol
CA	Certificate Authority
CAA	Certificate Authority Administrator
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy



Mobile Access Capability Package



Acronym	Definition
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CP	Capability Package
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
DAR	Data-At-Rest
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DM	Device Management
DN	Domain Name
DNS	Domain Name System
DOD	Department of Defense
DoE	Department of Energy
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
EST	Enrollment Over Secure Transport
EUD	End User Device
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards
FOTA	Firmware Over The Air
GOTS	Government Off-the-Shelf
GRE	Generic Routing Encapsulation
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alert
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol



Mobile Access Capability Package



Acronym	Definition
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS-IS	Intermediate System to Intermediate System
KM	Key Management
MA	Mobile Access
MDF	Mobile Device Fundamentals
MDM	Mobile Device Manager
MOA	Memorandum of Agreement
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPE	Non Person Entity
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
O	Objective
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPSEC	Operational Security
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
POC	Point of Contact
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
RD	Retransmission Device
RFC	Request for Comment
RIP	Routing Information Protocol
RSA	Rivest Shamir Adelman algorithm
SA	Security Association
SCRM	Supply Chain Risk Management
SDES	Session Description Protocol Security Descriptions
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Manager
SIP	Session Initiation Protocol



Mobile Access Capability Package



Acronym	Definition
SIPRNet	Secret Internet Protocol Router Network
SP	Service Packs
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
SSHv2	Secure Shell Version 2
T	Threshold
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TFFW	Traffic Filtering Firewall
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure
VoIP	Voice over Internet Protocol
VM	Virtual Machine
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access II

APPENDIX C. REFERENCES

CNSSI 1300	<i>CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy</i>	October 2009
CNSSI 4009	<i>CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.</i> http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2010
CNSSP 15	<i>CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems</i>	March 2010
CNSSD 505	<i>CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)</i>	March 2012
FIPS 140	<i>Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication</i> http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	<i>Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)</i>	March 2012
FIPS 186	<i>Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)</i>	July 2013
FIPS 197	<i>Federal Information Processing Standard 197, Advanced Encryption Standard (AES)</i>	November 2001



Mobile Access Capability Package



FIPS 201	<i>Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication</i> http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
IPsec VPN Client PP	<i>Protection Profile for IPsec Virtual Private Network (VPN) Clients.</i> http://www.niap-ccevs.org/pp	January 2012
NSA Suite B	<i>NSA Guidance on Suite B Cryptography (including the Secure Sharing Suite (S3)).</i> http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml	November 2010
RFC 2409	<i>IETF RFC 2409 The Internet Key Exchange (IKE).</i> D. Harkins and D. Carrel.	November 1998
RFC 3647	<i>IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> Internet Engineering Task Force	November 2003
RFC 3711	<i>IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).</i> M. Baugher and D. McGrew.	March 2004
RFC 4252	<i>IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol.</i> T. Ylonen and C. Lonvick.	January 2006
RFC 4253	<i>IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol.</i> T. Ylonen and C. Lonvick.	January 2006
RFC 4254	<i>IETF RFC 4254 The Secure Shell (SSH) Connection Protocol.</i> T. Ylonen and C. Lonvick.	January 2006
RFC 4256	<i>IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH).</i> F. Cusack and M. Forssen.	January 2006
RFC 4302	<i>IETF RFC 4302 IP Authentication Header.</i> S. Kent	December 2005
RFC 4303	<i>IETF RFC 4303 IP Encapsulating Security Payload.</i> S. Kent	December 2005
RFC 4307	<i>IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).</i> J. Schiller	December 2005
RFC 4308	<i>IETF RFC 4308 Cryptographic Suites for IPsec.</i> P. Hoffman	December 2005
RFC 4492	<i>IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).</i> S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006
RFC 4754	<i>IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA).</i> D. Fu and J. Solinas.	January 2007
RFC 5246	<i>IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2.</i> T. Dierks and E. Rescorla.	August 2008
RFC 5280	<i>IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.</i> D. Cooper, et. al.	May 2008



Mobile Access Capability Package



RFC 5759	<i>IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile.</i> J. Solinas and L. Ziegler.	January 2010
RFC 5996	<i>IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2).</i> C. Kaufman, et. al.	September 2010
RFC 6188	<i>IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.</i> D. McGrew.	March 2011
RFC 6239	<i>IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH).</i> K. Igoe.	May 2011
RFC 6379	<i>IETF RFC 6379 Suite B Cryptographic Suites for IPsec.</i> L. Law and J. Solinas.	October 2011
RFC 6380	<i>IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec).</i> K. Burgin and M. Peck.	October 2011
RFC 6460	<i>IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS).</i> M. Salter and R. Housley.	January 2012
RFC 6818	<i>IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.</i> P. Yee	January 2013
RFC 7030	<i>IETF RFC 7030 Enrollment over Secure Transport.</i> M. Pritikin, P. Yee, and D. Harkins.	October 2013
SP 800-53	<i>NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations.</i> Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	<i>NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.</i> E. Barker, et. al.	May 2013
SP 800-56B	<i>NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography.</i> E. Barker, et. al.	August 2009
SP 800-56C	<i>NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion.</i> L. Chen.	November 2011
SP 800-131A	<i>NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths.</i> E. Barker.	January 2011
SP 800-147	<i>NIST Special Publication 800-147, BIOS Protection Guidelines.</i> D. Cooper, et. al.	April 2011

APPENDIX D. END USER DEVICE IMPLEMENTATION NOTES

VPN EUDs:

The VPN EUD can be set up using a computing device with the user's applications, an Inner VPN Component, and an Outer VPN Component. The Inner VPN Component is a VPN Client residing on the same computing device as the user's applications. The Outer VPN Component can be a Dedicated Outer VPN Component or be a VPN Client on the same computing device as the user's applications (as shown



Mobile Access Capability Package



in Figure D-2). If a Dedicated Outer VPN component is utilized it must be connected to the computing device using Ethernet or wireless WPA2. When the Dedicated Outer VPN provides wireless connectivity to the computing device, the requirements in Section 12.9 must be followed. If all components are on the same device, virtual machines will be required to provide separate IP stacks for the Inner and Outer VPN Clients as noted in Figure D-2. A retransmission device will also be required in this case, unless, as noted in Section 4.1.3, the connection is to a Domestic Cellular Network, Government Private Wireless Network or a Government Private Cellular network. See Figure D-3.

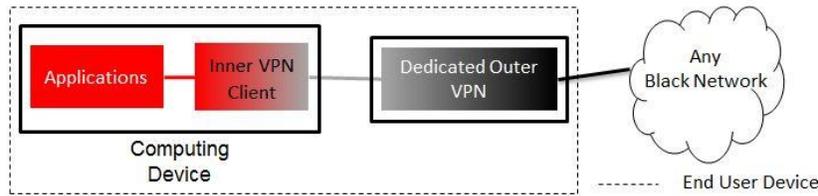


Figure D-1. VPN EUD with Inner VPN Client and Separate Outer VPN Gateway

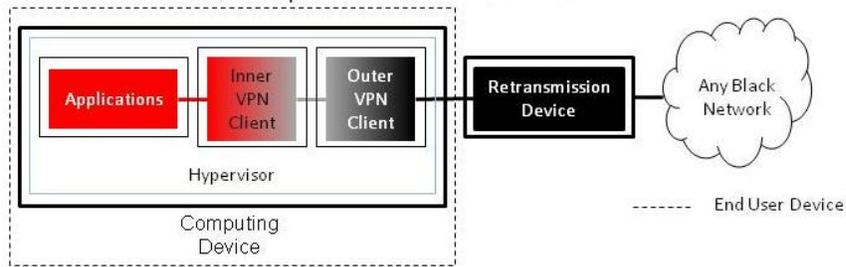


Figure D-2. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines with Retransmission Device

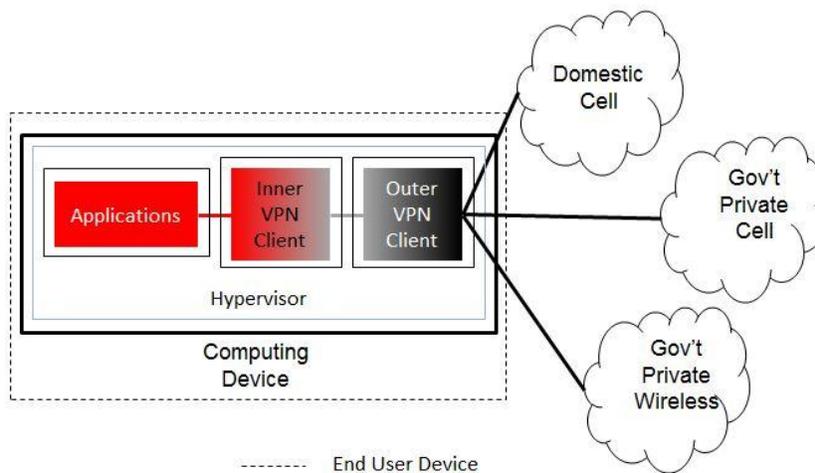


Figure D-3. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines without Retransmission Device



Mobile Access Capability Package



Transport Layer Security (TLS) End User Devices:

The TLS EUDs can be set up using up to two separate components. These components consist of the computing device and the VPN Component. The computing device sends and receives classified data. The Outer VPN Component is either a VPN Gateway or a VPN Client. Dedicated Outer VPN components are always physically separate from the computing device and are selected from the CSfC Components List (see Section 6.1.1). VPN Clients are selected from the IPsec VPN Client section of the CSfC Components List. The inner layer of encryption is always provided by an application on the computing device which terminates either TLS and/or SRTP. Each application installed on the computing device must be selected from the CSfC Components List. The CSfC Components List provides several sections for which customers can select the TLS Application including Web Browser, Email Client, and VoIP Application. Physical separation between encryption components provides a number of security advantages, but also is more difficult to implement due to the required hardware users require.

For TLS EUDs, each application installed on the computing device is responsible for terminating the inner layer of encryption. If a Dedicated Outer VPN component is utilized it must be connected to the computing device using Ethernet or wireless WPA2. When the Dedicated Outer VPN provides wireless connectivity to the computing device, the requirements in Section 12.9 must be followed.

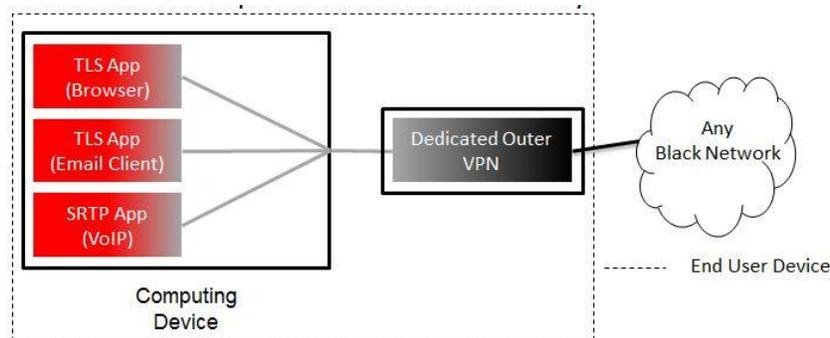


Figure D-4. TLS EUD with Separate Outer VPN Gateway

An Outer VPN Client can be installed within the same computing device as the TLS Applications which provide the inner layer of encryption as shown in Figure D-5. A retransmission device will also be required in this case, unless, as noted in Section 4.1.3, the connection is to a Domestic Cellular Network, Government Private Wireless Network or a Government Private Cellular network. See Figure D-6.



Mobile Access Capability Package

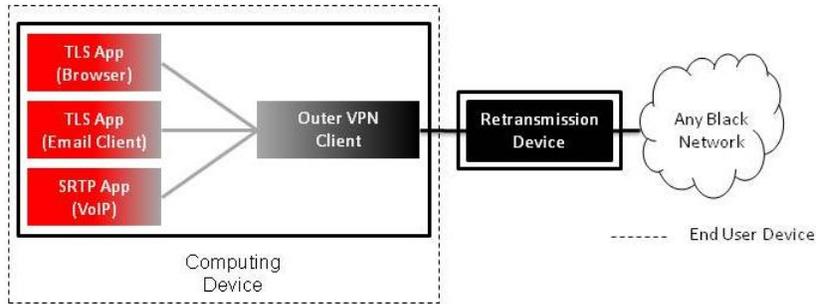


Figure D-5. TLS EUD with Integrated Outer VPN Client with Retransmission Device

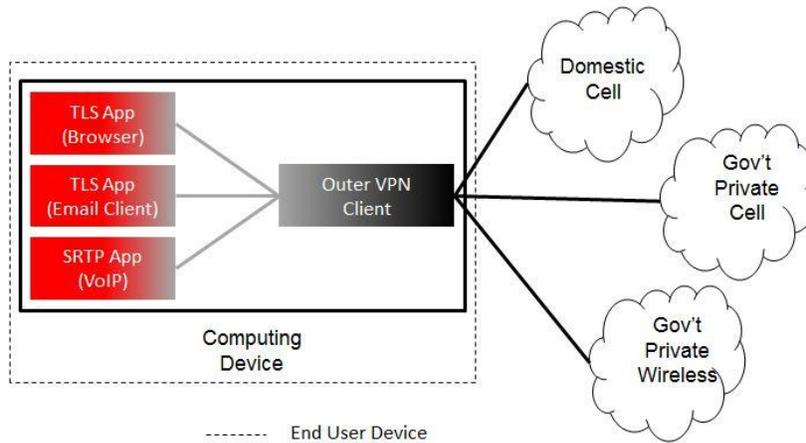


Figure D-6. TLS EUD with Integrated Outer VPN Client without Retransmission Device

Retransmission Devices:

A Government-owned Retransmission Device (RD) includes Wi-Fi Hotspots and Mobile Routers. On the external side, the RD can be connected to any type of medium (e.g., Cellular, Wi-Fi, SATCOM, Ethernet)



Mobile Access Capability Package



to gain access to the Wide Area Network. On the internal side the RD is connected to EUDs either through an Ethernet cable or Wi-Fi. See Figure D-7.

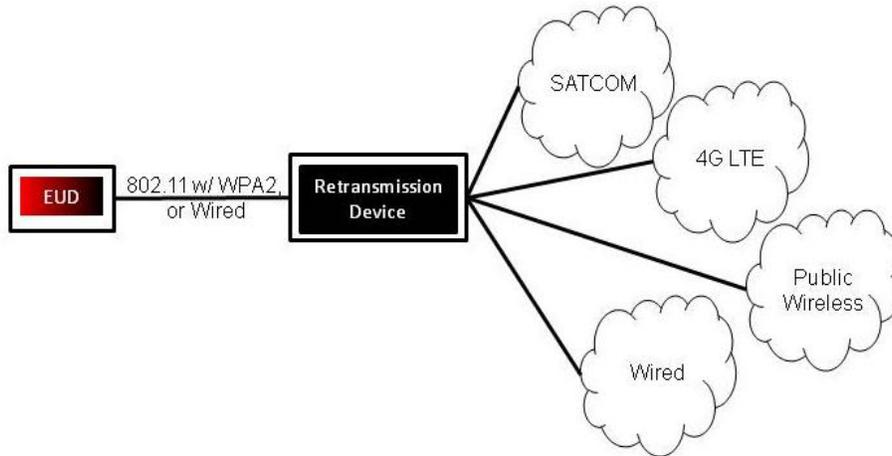
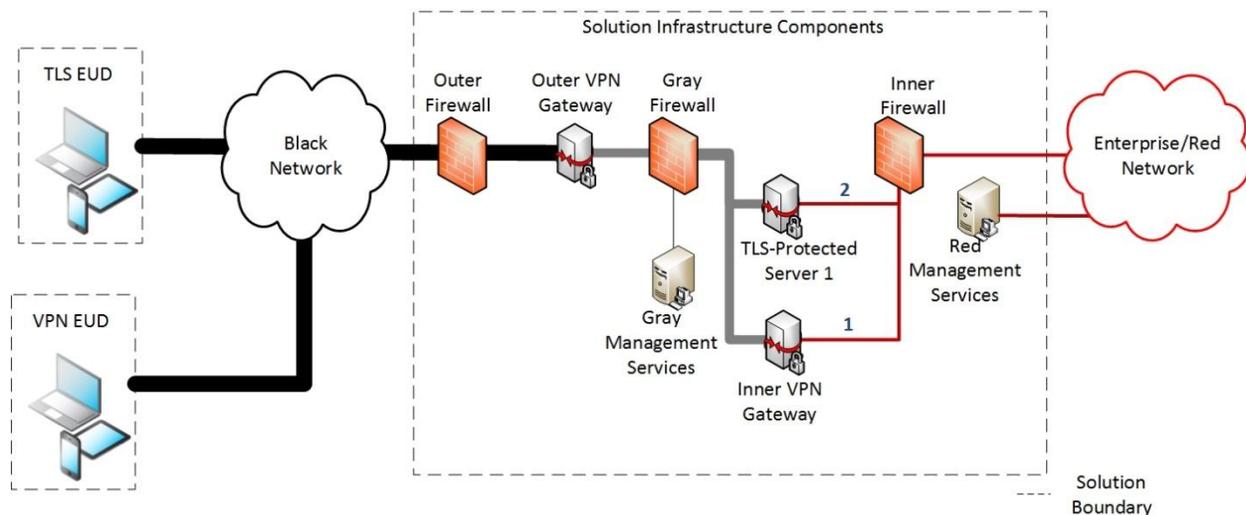


Figure D-7. Retransmission Device Connectivity

Solution Infrastructure supporting VPN and TLS EUDs

When supporting both VPN EUDs and TLS EUDs, the solution infrastructure will always include an Inner VPN Gateway between the Gray firewall and inner firewall (data flow 1 in Figure D-8). Additionally, the solution infrastructure will include one or more TLS-Protected Servers. The TLS-Protected Servers are also placed between the Gray firewall and inner firewall (data flow 2 in Figure D-8). Each Inner Encryption Component is independent and parallel to other Inner Encryption Components.

Figure D-8 below depicts an MA Solution which supports both TLS EUDs and VPN EUDs.





Mobile Access Capability Package



Figure D-8. Mobile Access Solution Infrastructure Supporting VPN and TLS EUDs

The following text describes each of the data flows depicted above.

1. The VPN Gateway terminates the inner layer of IPsec traffic for all VPN EUDs, and authenticates the EUD VPN client based on device certificates. There is a physical connection between the Gray firewall and the VPN Gateway and between the VPN Gateway and the inner firewall.
2. The TLS-Protected Server is placed between Gray firewall and inner firewall. The TLS-Protected Server terminates the inner layer of TLS traffic for one or more of the services available to TLS EUDs. The TLS-Protected Server could also be a Session Border Controller which terminates SRTP traffic and relays it to the appropriate destination in the Red network. The TLS-Protected Server authenticates the EUD's TLS client based on user or device certificates. There is a physical connection between the Gray firewall and the TLS-Protected Server and between the TLS-Protected Server and the inner firewall. This connection is in parallel with the VPN Gateway such that the TLS-Protected server is not dependent on the Inner-VPN Gateway to reach the Gray firewall or the inner firewall.

TACTICAL SOLUTION IMPLEMENTATIONS

Although the majority of customers instantiating solutions based on the MA CP will be utilized for Strategic or Operational Environments, some organizations may deploy the MA CP in Tactical Environments. These Tactical Environments include a specific set of Size, Weight, and Power (SWaP) constraints not found in traditional environments.

Organizations intending to deploy an MA CP Solution for Tactical Environments may utilize this Appendix, which accommodates the SWaP constraints unique to their environment. This Appendix may only be utilized to protect Tactical Data classified as SECRET or below. The CP follows CNSSI 4009, which defines Tactical Data as "Information that requires protection from disclosure and modification for a limited duration as determined by the originator or information owner." In addition to protecting Tactical Data, organizations that register their solution using this Appendix must be deployed at the Tactical Edge. The CP also follows CNSSI 4009, which defines the Tactical Edge as "The platforms, sites, and personnel (U. S. military, allied, coalition partners, first responders) operating at lethal risk in a battle space or crisis environment characterized by 1) a dependence on information systems and connectivity for survival and mission success, 2) high threats to the operational readiness of both information systems and connectivity, and 3) users are fully engaged, highly stressed, and dependent on the availability, integrity, and transparency of their information systems."

If an organization's planned solution meets the two above criteria then their solution may be registered utilizing the requirement accommodations in this Appendix. The MA CP Registration form must explicitly state that the solution is being utilized in Tactical Environments and provide justification on how the above criteria are met. In general, customers registering with this Appendix will be deployed in support of Battalion and below (or equivalent) unit structure. Typically, these Tactical Environments are located in austere environments where communication infrastructure is generally limited. Due to the lack of



Mobile Access Capability Package



existing communication infrastructure, the Tactical Environments are also generally characterized by the use of Government owned Black Infrastructure (Government Private Wireless Networks and/or Government Private Cellular Networks).

The below table may be utilized by customers meeting the above criteria when configuring, testing, registering, and operating their Mobile Access Solution. Any questions on the use of this Appendix should be directed to mobile_access@nsa.gov and csfc@nsa.gov.

Table 31. Tactical Implementation Requirements Overlay

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-17	The Outer firewall, Outer VPN Gateway, Gray firewall, Inner Encryption Component, and Inner firewall shall use physically separate components, such that no component is used for more than one function (see Figure 1).	VI, TI	O	MA-TO-1
MA-TO-1	The Outer VPN Gateway shall be physically separate from the Inner Encryption Components	VI, TI	T	MA-PS-17
MA-EU-12	Users of EUDs shall successfully authenticate themselves to the services they access on the Red network using an AO approved method.	VE, TE	O	
MA-EU-13	Red network services shall not transmit any classified data to EUDs until user authentication succeeds.	VE, TE	O	
MA-MR-5	Each IDS in the solution shall be configured to send alerts to the Security Administrator.	All	O	
MA-MR-7	The organization shall create IDS rules that generate alerts upon detection of any unauthorized destination IP addresses.	All	O	
MA-DM-14	The Outer VPN Gateway and solution components within the Gray network shall forward log entries to a SIEM on the Gray Management network (or SIEM in the Enterprise/Red Network if using an AO approved one-way tap) within 10 minutes.	VI, TI	O	