COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

EUD Composition Guidance Addendum 2.0

Draft 1.0

Version 2.0 Draft 1.0
1 September 2026

19 # CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) EUD Composition Guidance Addendum	2.0 Draft 1.0	1 September 2026	Composed Hardware-Separated EUD Composition Guidance Addendum
Commercial Solutions for Classified (CSfC) EUD Composition Guidance Addendum	1.0.0	5 May 2023	Initial Draft of the EUD Composition Guidance

20

21

DRAFT

Table of Contents

DRAFT

DRAFT

Table of Figures

DRAFT

List of Tables

DRAFT

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency's (NSA) Cybersecurity Directorate (CSD), publishes Capability Packages (CPs) to provide configurations that empower NSA 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.

This document is an Addendum to the *CSfC Mobile Access (MA), Campus Wireless Local Area Network (CWLAN), and Data-at-Rest (DAR) CPs* that convey a structural changes to the End User Device (EUD) to clarify the usage of technologies, product selections, and other changes. This addendum is provided to allow for the customer base and interested parties to comment on these changes before they are made within the above-mentioned CPs and released as minor increments to these CPs. This addendum will not be released past draft and only exists for customer awareness of changes to upcoming CPs.

While CSfC encourages industry innovation; trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a National Information Assurance Partnership (NIAP)-validated component in a CSfC solution may invalidate its certification and require a revalidation process. To avoid delays, customers and Integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/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, the NSA's CSfC Program Management Office (PMO) 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, configuring the component in a manner different from its NIAP-validated configuration and modifying the Original Equipment Manufacture's code (to include digitally signing the code).

2 PURPOSE AND USE

This Addendum provides high-level reference architecture and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List, available on the CSfC web page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program), to compose a Hardware-Separated EUD to meet the requirement needs of the MA, CWLAN, and DAR CPs. As described throughout this Addendum, customers must ensure that the components selected from the CSfC Components List provide the necessary functionality for the selected capabilities. To successfully implement a solution based on the specified CPs, all Threshold (T) Requirements, or the corresponding Objective (O) Requirements applicable to the selected capabilities, must be implemented.

DRAFT

Please provide comments on the usability, applicability, and/or shortcomings to your NSA Client Advocate and the Addendum Maintenance Team at mobile_access@nsa.gov. CSfC solutions must also comply with the Committee on National Security Systems (CNSS) Policies and Instructions. Any conflicts identified between this Addendum and CNSS or local policy should be provided to the Addendum Maintenance Team.

For information on Cross Domain Solutions (CDS) contact the National Cross Domain Strategy Management Office (NCDSMO) at ncdsmo@nsa.gov.

Customers and Integrators must adhere to all applicable data transfer policies for their organization when designing and implementing these capabilities within their CSfC solution architecture. For example, Department of War (DoW) customers must follow DoDI 8540.01, Cross Domain (SD) Policy", when deploying a CDS within a CSfC solution and if any discrepancies found between the guidance in this document and DoDI 8540.01 should be reported accordingly.

3 LEGAL DISCLAIMER

This Addendum is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties or merchantability and fitness for a particular purpose are disclaimed. In no event must the U.S. 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 Addendum, even if advised of the possibility of such damage.

The user of this Addendum agrees to hold harmless and indemnify the U.S. 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 third parties, and infringement or other violations of intellectual property or technical data rights.

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

DRAFT

4 OVERVIEW

This Addendum revises and expands upon the current Composed EUD guidance and clarifies the concept of a Hardware-Separated EUD. The core concept of Hardware-Separated EUDs is that critical functions such as transport, encryption, and the processing of classified data are separated into dedicated hardware components. The objective is to provide an EUD that separates high-risk functionality inherent in the CSfC EUDs as defined in the CSfC Risk Assessment.

Within the CSfC architecture, particularly the MA CP, the concept of multiple components making up a single EUD already exists. This concept is exemplified by the Retransmission Device (RD) and the Dedicated Outer (DO) Virtual Private Networks (VPNs) which can be paired with a traditional EUD. This approach allows both functionality and risk to be shifted to a separate component rather than the EUD, or enable a separate component to perform a function the EUD is incapable of performing. This concept can be further refined to enhance the security of an EUD or to allow EUDs that cannot meet the requirements placed on traditional EUDs such as a laptop, smartphone, tablet, or computer.

Table 1 summarizes the EUD types described in this document. This document focuses on the concept of the Hardware Separated EUD.

Table 1. EUD Summary

Sub-Component	Description	Note
MDF EUDs	An EUD built to function within the constraints of a typical MDF system	Normally encompasses smartphones and Tablets. All in one device
Composed EUDs	An EUD built to function within the constraints of a typical Operating System (OS) and Hardware Platform	A device must be composed from multiple CSfC listed components
Virtualized EUD: Type 1 hypervisor with Hardware Abstraction	An EUD built around a Type 1 hypervisor with Hardware Abstraction Capabilities to separate the critical functions into separate virtual instances	Offers more usability and increases the security by added hardware abstraction.
Hardware-Separated EUD	An EUD with critical functions (Transport, Encryption, and Red Components) separated into dedicated hardware components	High risk functions are physically separated out into the separate hardware of the EUD

Additionally, this Addendum will further codify and solidify the requirements for MA CP RD. This is intended to provide clarity to the CSfC customer base regarding which RDs are suitable for use within the MA CP and provide enhanced security requirements for the RD. This includes collaboration with NIAP on the development of an RD Protection Profile (PP) that defines both the required security and

DRAFT

management for these devices. Additionally, this PP offers an alternative method for evaluation of DOs for MA and CWLAN CPs.

4.1 HARDWARE-SEPARATED EUD

Within the CSfC architecture, particularly in the MA CP, the concept of multiple components comprising a single EUD already exists. This concept is exemplified by the RD and the DO VPNs when paired with a traditional EUD. This transfers both functionality and risk to separate components other than the EUD, or enables a separate component to perform a function the EUD is incapable of performing. The Hardware-Separated concept can be leveraged to further enhance the security of an EUD or allow for EUDs that cannot meet the requirements placed on a traditional EUD such as a smartphone, tablet, laptop, or computer.

This concept mitigates risk to the EUD by physically separating the three logical information boundaries within CSfC: Red, Gray, and Black. These architectures are also being considered as the rapidly evolving threat environment of artificial intelligence-based cyber security research. The Black portion, or RD, of an EUD, handles the connection to, and all communication over, the untrusted network (i.e., public Internet). This is currently exemplified by the RDs in the MA CP. The Gray portion, or DO, of the EUD is the first cryptographic boundary which hosts the Outer Encryption Component, such as the DOs within the MA CP and CWLAN CP. The Red portion, or Dedicated Inner and Red Compute, of the EUD contains both the secondary cryptographic boundary and the user space. The expected form of the Red Compute is either an MDF EUD or a Composed EUD. The Composed Hardware-Separated EUD design is the preferred EUD within CSfC Solutions.

For more information and details on Hardware Separated EUD see Section 5.

4.2 RETRANSMISSION DEVICES

An RD is a government owned network device whose primary purpose is to provide network connectivity to the EUD or DO and to provide a layer of hardware isolation between the Black Transport Network (i.e., the internet) and an EUD or DO. Most EUDs are capable of connecting to Black Transport Networks directly but the RD is meant to provide isolation from the cellular networks or other such wireless networks and the EUD. The EUD or DO is meant to be directly connected through a hard-wired connection such as Ethernet or Ethernet over USB. The connection between the RD and the Black Transport Network may be any wireless or wired connection approved by the Authorizing Official (AO).

The CSfC Program has long mandated the use of RDs to further enhance the security of MA CP EUDs ensuring that high-risk functions are conducted by the RD. Traditionally, the RD has been considered a device outside the CSfC Security boundary but one that provides critical network connectivity to the EUD. Additionally, the program has introduced a number of security requirements to the RD, leaving it to the customers to select an RD suitable for their mission without product-selection constraints applied to other components such as VPN Gateways or EUDs. In partnership with NIAP, the CSfC Program is

DRAFT

developing a NIAP PP that will define the security requirements for an RD and also serve as an alternative path for DOs.

For additional information and details on RDs, see Section 5.3.

4.3 Managing Retransmission Devices and Dedicated Outers from the EUD

With the increased emphasis on using DOs within the CPs, the control boundary of the EUD expands across multiple platforms beyond the limitation of an individual EUD. As a result, multiple options are needed for managing both the DO and RDs within the CP. The first option is for a local administrator to manage the DOs and RDs through a dedicated management interface. The second option is for the DO to be managed and monitored from the Gray Network, either through a Transport Layer Security (TLS) connection or directly from the Outer Encryption Components, as detailed in Sections 5.2.2 and 5.2.3. The RD can be managed in a similar manner, but this would occur on an AO-approved platform from the Black Network. This second option requires both the RDs and DO to be operational. A third option is a dedicated KVM (Keyboard, Video, Mouse) placed within the EUD to allow the local user to configure the RD and DO, as detailed in Section 5.4.1. Finally, if an EUD relies on the virtualization requirements and a controlled interface, then it can communicate directly with the DO or, if no DO is in place, the RD as detailed in Section 6.

4.4 EUD Provisioning

Provisioning is the process through which EUDs are initialized before first use, wherein, an EUD is transitioned from its default settings and provisioned to a fully operational CSfC EUD. This process includes, but is not limited to, removing default applications and certificates, installing required applications, installing encryption clients and profiles, installing CSfC Certificates, and performing specific actions required to lock down the EUD. This process occurs when an EUD is initially brought into a CSfC Solution and can be repeated as needed through a reprovisioning process. The EUD provisioning process is required in all CPs that include EUDs, DAR, MA, and CWLAN. This document aims to better unify the requirements across all CPs while retaining the specific requirements unique to each CP. For more details, see Section 7.

4.5 Multiple Security Levels

All Data-in-Transit (DiT) CPs provide options for supporting multiple Inner Encryption Components to a single Outer Encryption Component to handle multiple classifications. For the CWLAN and MA CPs, a key security concern is ensuring separation of EUDs as their tunnels transit the Gray Data Plane to connect to the Inner Encryption Component. The Outer Encryption Component must identify every EUD and route it to the correct network to separate the EUDs by classification level. This separation of EUDs at different classification levels must be enforced by both the Outer Encryption Component and the Gray Firewall through either cryptographic means (IPsec VPN or Datagram Transport Layer Security (DTLS)) or physical means (separate interfaces).

DRAFT

5 HARDWARE-SEPERATED EUDS

Within the CSfC architecture, particularly the MA CP, there is the concept of multiple components making up a single EUD. This concept is exemplified by the RD and the DO VPNs, which can be paired with a traditional EUD. This allows for EUDs that cannot operate the Inner Encryption to still be used within CSfC, or allow the risk associated with the Red Compute to be passed along to another dedicated component.

The Red Compute Hardware and DO are objective design features within a CSfC Solution and are not required for customer implementation. This concept can be further expanded to enhance the security of an EUD or allow for EUDs that cannot meet the requirements placed on traditional EUDs, such as laptops, smartphones, tablets, or computers.

5.1 RED COMPUTE

The Red Compute is, for all intents and purposes, a traditional CSfC EUD and has two primary purposes: conducting the inner layer of encryption and processing classified information. All requirements that apply to traditional CSfC EUDS, also apply to Red Compute.. For a quick summary, see Table 2 below.

Table 2. Red Compute Components

Sub-Component	Description	CSfC Components for Red Compute	Note
Mobile Device Fundamentals (MDF) EUDs	An EUD built to function within the constraints of a typical MDF system	• MDF EUD	Normally encompasses smartphones and tablets. All in one device
Composed EUDs	An EUD built to function within the constraints of a typical OS and Hardware Platform	• General Purpose Computing Platform • Dedicated Security Component (Optional) • General Purpose OS • IPsec VPN Client or TLS Client • Hardware Full Drive Encryption or Software Full Drive Encryption	A device must be composed from multiple CSfC listed components
Virtualized EUD	An EUD built around a Type 1 hypervisor with Hardware Abstraction Capabilities to separate the critical functions into separate virtual instances	• General Purpose Computing Platform • Dedicated Security Component (Optional) • Client Virtualization • IPsec VPN Client or TLS Client • Hardware Full Drive Encryption or Software Full Drive Encryption	Offers more usability and increases the security by added hardware abstraction

DRAFT

Potential use cases for a composed Hardware-Separated EUD include, but are not limited to, a laptop solution with a physically separate Red Compute/Inner VPN, a DO Encryptor, and an RD in a single chassis; or a mobile phone solution within a sleeve housing an RD, or a mobile phone solution within a sleeve housing both the DO Encryptor and an RD.

5.1.1 DATA AT REST

The goal of the DAR solution, according to the DAR CP, is to protect classified data when the EUD is powered off or unauthenticated. "Unauthenticated" is defined as the state of the EUD before a user presents their credentials (i.e., password, tokens, etc.) and are validated by both layers of the DAR solution. The DAR solution is composed of dual encryption layers, an outer and an inner layer. The outer layer is the layer authenticated to first, followed by the inner layer. The data owner determines the specific data that must be protected.

When a Hardware-Separated EUD is being used in conjunction with the DAR CP, only the Red Compute is treated as the EUD.

5.1.2 MOBILE ACCESS AND WLAN RED COMPUTE REQUIREMENTS

Red Compute devices must meet all EUD requirements, with the exception of any requirements that relate directly to the Outer Encryption, since those requirements are being managed by the DO. In addition, the Red Compute must meet all product-selection requirements, as if it were the EUD, and meet all respective EU requirements.

Table 3. MA Red Compute EUD Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-22	The EUD must disable all wireless interfaces (e.g., Bluetooth, Near Field Communication (NFC), Cellular, 802.11) via Airplane mode.	All	T	MA-EU-83 MA-EU-85
MA-EU-61	Withdrawn			
MA-EU-83	All wireless interfaces must be disabled on the Red Compute platform via one of the following: • firmware disablement or • physical/hardware disablement	All	O	MA-EU-22, or MA-EU-85
MA-EU-84	The EUD screen must lock after 15 minutes or less of inactivity.	CE, VZ, HS	T=O	MA-EU-40
MA-EU-85	The EUD must disable all wireless interfaces (e.g., Bluetooth, NFC, Cellular), except the Wi-Fi Interface used to connect to a Government Private Wireless or Wireless RD through software or physical means.	All, WC	T=O	MA-EU-22, or MA-EU-83

DRAFT

For a WLAN CP EUD, the wireless functionality, which is a core capability and trusted layer of the encryption, is moved onto a separate DO WLAN. As a result, the Red Compute must have all wireless interfaces disabled and a wired interface enabled so that the EUD can leverage the DO WLAN for Wireless Communications to the trusted network.

Table 4. WLAN Red Compute EUD Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-1	The EUD or DO must restrict configuration (Service Set Identifier (SSID) and authentication mechanism) of authorized WLANs to authorized administrators.	T=O	
WLAN-EU-20	The EUD must have all network and wireless interfaces disabled except for 802.11 while in operation.	T=O	WLAN-EU-49
WLAN-EU-36	The EUD or DO must be configured to only permit connections to allowlisted SSIDs.	T=O	
WLAN-EU-37	The EUD or DO must be configured to only permit connection to SSIDs using certificates signed by the Outer (Certificate Authority (CA).	T=O	
WLAN-EU-38	The EUD must only display allowlisted SSIDs to the user.	O	
WLAN-EU-49	The EUD must have all wireless interfaces disabled, except for 802.11 while in operation.	T=O	WLAN-EU-20
WLAN-EU-50	All unused EUD wireless and wired interfaces must be disabled via software (i.e. Airplane mode).	T	WLAN-EU-51
WLAN-EU-51	All unused EUD wireless and wired interfaces must be disabled via one of the following: • firmware disablement • physical/hardware disablement	O	WLAN-EU-50
WLAN-EU-52	If using a DO WLAN, the DO WLAN must be the Outer Layer of encryption, and the VPN client on the Computing Device will be the Inner Layer of encryption.	T=O	

5.2 DEDICATED OUTER (OUTER ENCRYPTION COMPONENT)

A DO is a separate component that can be used as the Outer Encryption for an EUD. These DOs are normally small travel routers or similar network gear. There are currently two different options for DOs:

- DO VPN
- DO WLAN

DRAFT

Table 5. DO Options

Types of DOs	Description	CSfC Components for DO	Note

DO VPN	An MA DO which connects to the Outer VPN Gateway	• VPN Gateway
		• Pending RD Component
		• Virtualized EUD
		  ○ VPN Gateway or IPSec Client
		• Composed EUD
		  ○ IPSec Client
		• MDF EUD
		  ○ IPSec Client	

DO WLAN	A CWLAN DO that directly connects to the authorized WLAN Access System	• WLAN Access System
		• Pending Retransmission device Component
		• Virtualized EUD
		  ○ WLAN Access System or WLAN Client
		• Composed EUD
		  ○ WLAN Client
		• MDF EUD
			Does not require an RD

5.2.1 Dedicated Outer and Red Compute Connectivity

Since the DO and Red Compute are two physically separated devices connected through a wired connection, additional security considerations must be considered for that connection. The DO must only support a single classification of EUD, though it can support more than a single EUD. Both the DO and the connected device must be physically handled as if classified to the classification which the Red Compute device processes. For additional security, the DO should either implement port security on the interface between the Red Compute and the DO or implement 802.1X. For single form factor EUDs that physically host the Red Compute and DO, these additional security mechanisms are not necessary.

5.2.2 Monitoring Dedicated Outers

The DO is capable of logging events such as the establishment and termination of VPN tunnels, the establishment and termination of Wi-Fi connections, and other relevant security and configuration events.

Once generated, device logs are then forwarded to the Gray Data collection server using an existing Outer Encryption tunnel, establishing a layer of encryption using SSHv2, IPsec, TLS 1.2 or later, Media Access Control Security (MACsec), or DTLS.

DRAFT

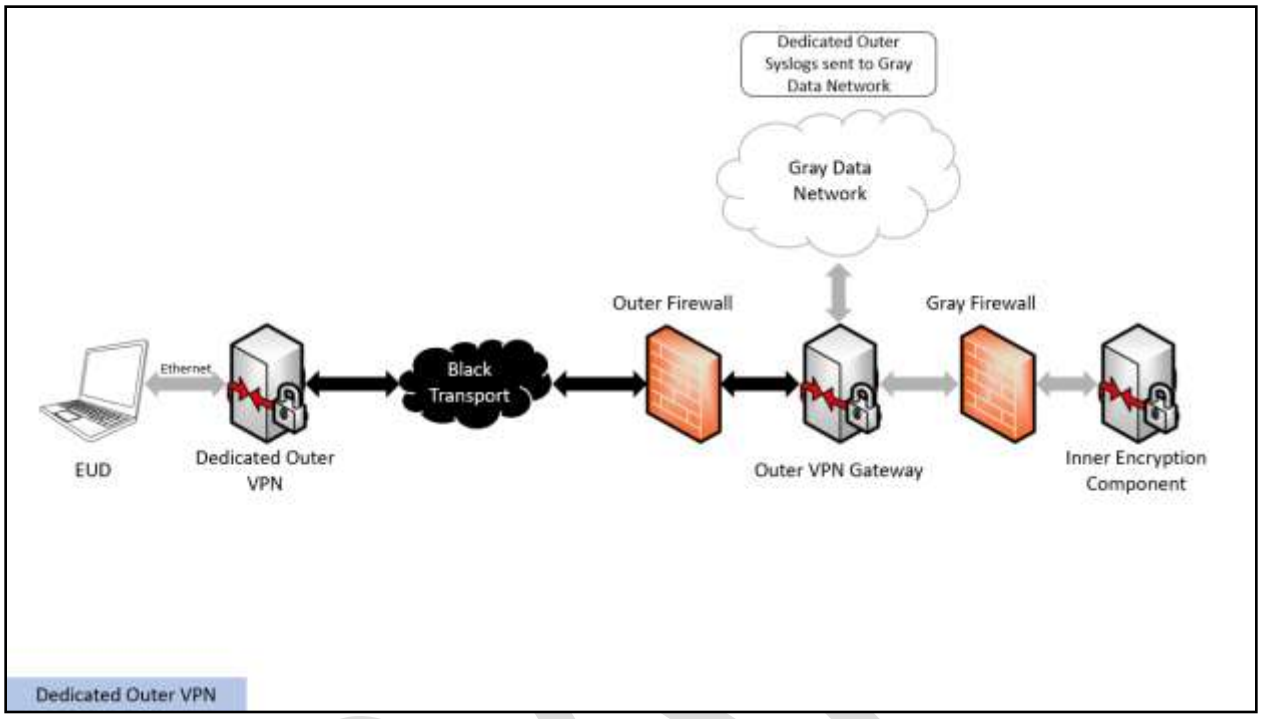


Figure 1. DO VPN Monitoring

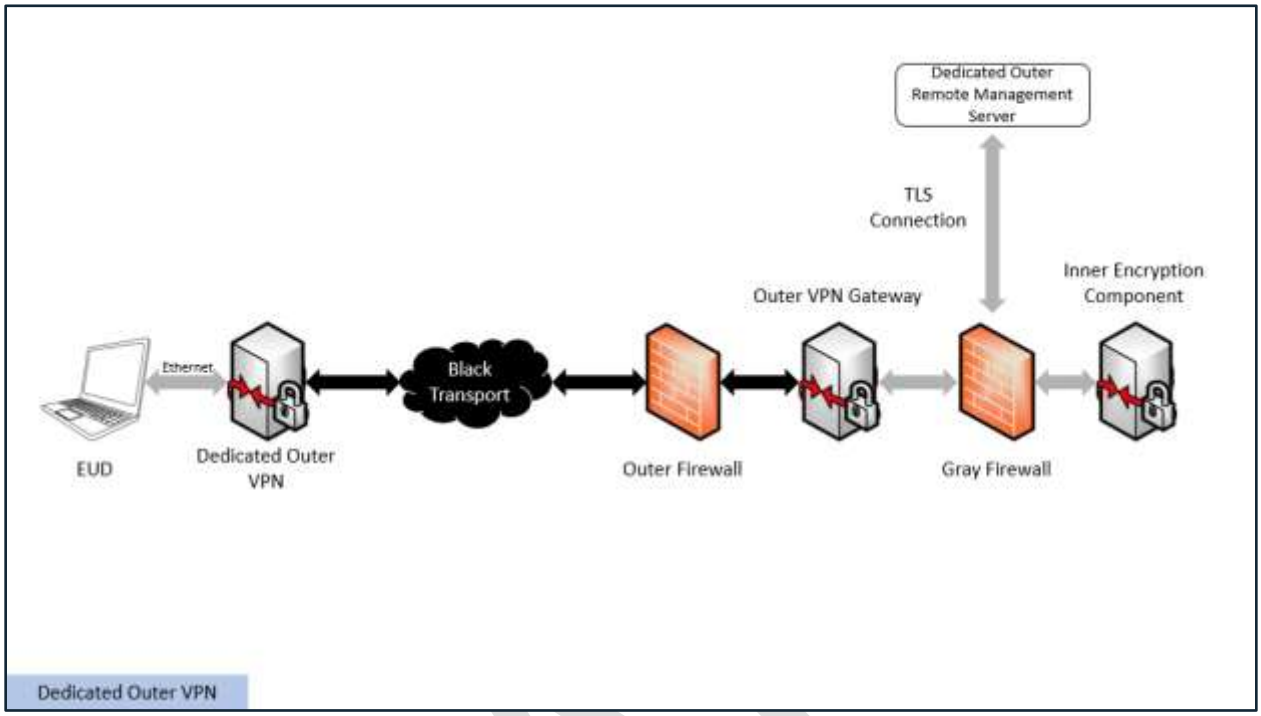
For more information see *CSfC Continuous Monitoring Annex 2.0.0 Draft 1.0.*

5.2.3 MANAGING DEDICATED OUTERS

A DO can be managed through a local interface by an authorized administrator through a management interface. Another acceptable method for managing a DO is remote managing of DOs through the Gray Network.

Local management of the DO is not intended for the user to manage the DO, but instead, for a security administrator to manage the device. This management is expected to be done in a secure location and only occur as necessary, such as when certificates need to be renewed or for system updates.

The remote management of the DO occurs either through the Outer Encryption Component or another TLS Protected Server on the Gray Data Plane. When managing the DO remotely, this control channel must first transit through the Outer Encryption, IPsec Tunnel, or Wi-Fi connection. Then, TLS or DTLS must be used to establish a connection to the Outer Encryption Component or TLS Protected Server on the Gray Data Plane.



344

345 **Figure 2. DO VPN Remote Management**

346 ### 5.2.4 DEDICATED OUTER VPN

347 A DO VPN is a separate component used as the Outer VPN for a Composed Hardware-Separated EUD.
348 The DO VPN must be physically connected to the Red Compute through a wired connection. The DO VPN
349 must either be physically connected through a wired connection to either an RD or other untrusted
350 Black interface.

351

DRAFT

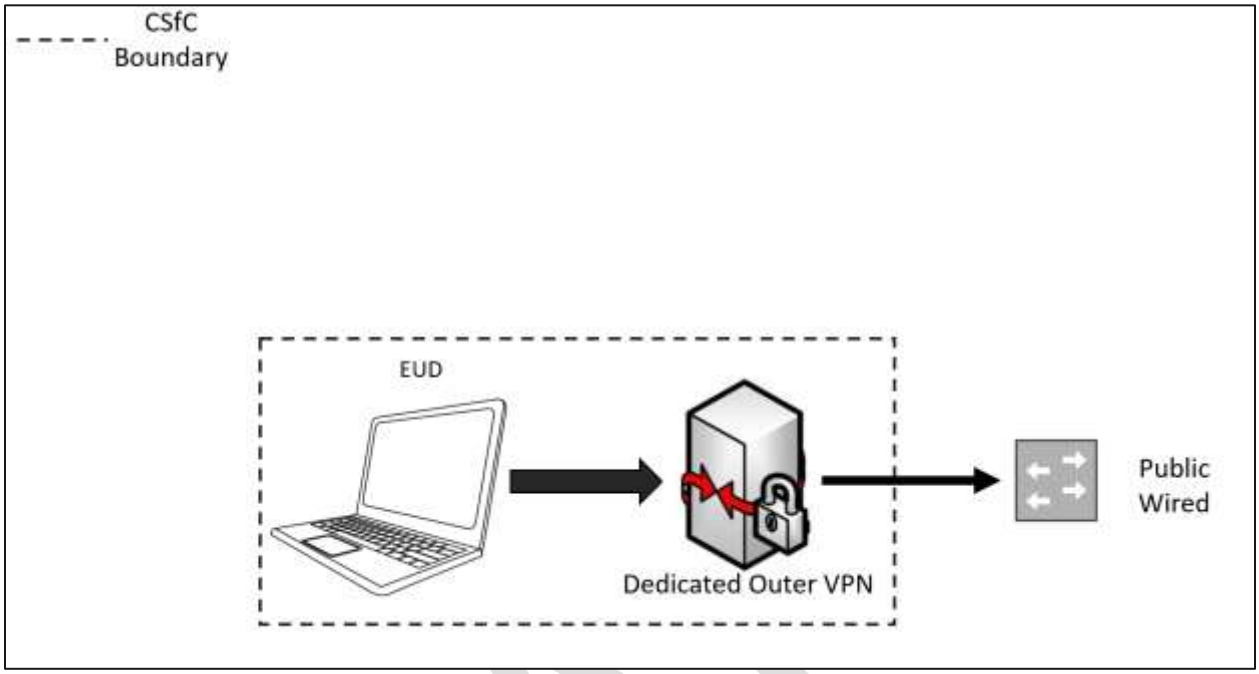


Figure 3. DO VPN

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

A DO VPN is chosen from the CSfC Components List as one of the following:

- An IPSec VPN Gateway
- A Composed DO made up of the following components:
  - General Purpose Operating System (GPOS)
  - General Purpose Compute Platform (GPCP)(Optional)
  - IPSec VPN Client
- Or an RD with IPSec Encryption functionality

Additionally, it is recommended that the DO VPN include either platform encryption or a full drive encryption chosen from the CSfC Components list, however, this remains an objective design feature.

369 **Table 6. DO VPN Component Selection**

DO VPN	Description	CSfC Components List	Note
IPsec VPN Gateway	A VPN Gateway that is used for site-to-site encryption for connection to the Outer VPN Gateway	• IPSec VPN Gateway	
Composed DO VPN	A Composed DO made up of CSfC Components running the Outer VPN Client	• General Purpose OS • General Purpose Compute Hardware (Optional) • IPSec VPN Client • Hardware or Software Full Drive Encryption (Optional)	
Retransmission Device/w IPSec VPN	An RD that is used for site-to-site encryption for connection to the Outer VPN Gateway	• RD-DO	Pending PP

370

371 The following table is a list of component requirements that will be appended or changed in the MA CP
372 as part of the Composed Hardware-Separated EUD Composition update.

373 **Table 7. DO VPN Requirements**

Req #	Requirement Description	Threshold/ Objective	Alternative
MA-PS-27	If the solution uses a DO VPN as part of an EUD, it must be selected from the list of IPsec VPN Gateways or RD-DO on the CSfC Components List.	T=O	MA-PS-41
MA-PS-41	If the solution uses a DO VPN as part of an EUD, it must be composed from components from the GPOS or hypervisor with an IPSec VPN Client from the CSfC Components List.	T=O	MA-PS-27
MA-DO-13	The DO VPN must be managed over a dedicated wired interface.	T=O	MA-DO-20
MA-DO-17	All Red Compute or EUDs must connect to the DO VPN with a wired connection.	T=O	
MA-DO-20	The DO VPN must be remotely administered from the Gray Data Plane either by the Outer VPN Gateway it is connected to or a dedicated TLS server.	T=O	MA-DO-13
MA-DO-21	The DO VPN must be administered over a secure connection (i.e., SSH, TLS, DTLS, IPSec).	T=O	
MA-DO-22	The DO VPN must strip and replace the Data Link Layer protocol headers between the DO Encryptor and the Red Compute platform.	T=O	
MA-DO-23	The DO VPN must have one layer of Platform Encryption.	O	
MA-DO-24	The DO VPN must be connected with a wired interface to the RD or Black Transport Network.	T=O	

DRAFT

MA-DO-25	The DO VPN and EUD must authenticate each other through MAC address, IP Address or 802.1X connection before the EUD establishes the connection.	T=O	

5.2.5 DEDICATED OUTER WLAN

The DO WLAN handles the Wi-Fi connectivity for a Composed Hardware-Separated EUD that is either incapable of operating a Wi-Fi connection or to pass along the risk of a Wi-Fi connection to another component. These DOs are normally small travel routers, Wi-Fi Access Points, or similar networking gear. Another option for a DO WLAN is to designate it as a component of a Composed Hardware-Separated EUD. The DO WLAN, included as part of the Composed Hardware-Separated EUD, must be physically connected to the Red Compute platform using a wired connection. DO WLANs are dedicated to a single security level and can only provide the Outer WLAN layer for Red Compute platforms connecting to a Red Network of the same security level.

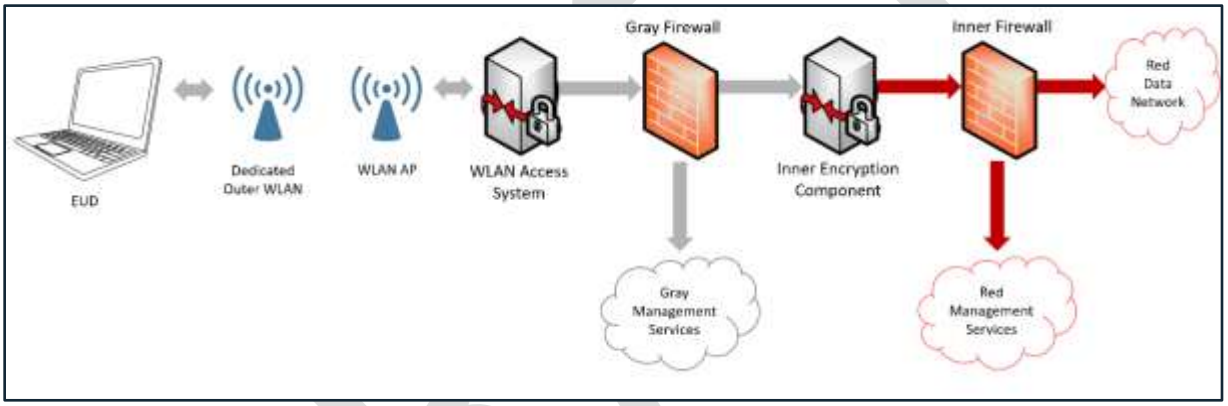


Figure 4. DO WLAN

When a DO WLAN is included as part of the Composed Hardware-Separated EUD, it provides configuration and enforcement of network packet handling rules for the Outer layer of encryption. When the DO WLAN is included as part of the Composed Hardware-Separated EUD, the DO WLAN's OS must be selected from the *OS* section of the CSfC Components List. When the DO WLAN is included as part of the Composed Hardware-Separated EUD, the hardware must be selected from the *Hardware Platform* section of the CSfC Components List.

A DO WLAN is selected from the CSfC Components List as one of the following:

- A WLAN Access System
- An MDF EUD
- A Composed DO WLAN made up of the following components:
  - GPOS
  - GPCP(Optional)
  - WLAN Client

- Or an RD with WLAN Client Functionality

Additionally, it is recommended that the DO WLAN has either platform encryption or a full drive encryption selected from the CSfC Components list. This remains an objective design feature.

Table 8. DO WLAN Component Selection

DO WLAN	Description	CSfC Components List	Note
WLAN Access System	A WLAN Access System acting as a WLAN Client to connect to the WLAN Access System	• WLAN Access System	
MDF EUD	An MDF EUD running the WLAN Client to connect to the WLAN Access System	• MDF EUD	WLAN Client is built into MDF
Composed DO WLAN	A Composed DO composed of CSfC Components running the WLAN Client to connect to the WLAN Access System	• General Purpose OS • General Purpose Compute Hardware (Optional) • WLAN Client • Hardware or Software Full Drive Encryption (Optional)	
RD/w WLAN Client	An RD acting as a WLAN Client to connect to the WLAN Access System	• RD- DO WLAN	Pending PP

5.2.5.1 Dedicated Outer WLAN Component Requirements

The following table is a list of product selection requirements that will be appended or modified to the CWLAN CP as part of the Composed Hardware-Separated EUD Composition update.

Table 7. DO WLAN Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-PS-3	The products used for any WLAN Client must be selected from the list of Mobile Platforms on the CSfC Components List or an OS that is listed on the CSfC Components List for WLAN Clients.	T=O	WLAN-PS-21 Or WLAN-PS-26
WLAN-PS-21	If the solution uses a DO WLAN as part of an EUD, it must be selected from the list of WLAN Access Systems, MDF EUDs or RD-DOs on the CSfC Components List.	T=O	WLAN-PS-3 or WLAN-PS-26
WLAN-PS-26	If the solution uses a DO WLAN as part of an EUD, it must be composed of GPOS and WLAN Client components from the CSfC Components List.	T=O	WLAN-PS-3 or WLAN-PS-21

DRAFT

WLAN-WO-7	The DO WLAN must be managed over a dedicated wired interface.	T	WLAN-WO-8
WLAN-WO-8	The DO WLAN must be remotely administered from the Gray Data plane either by the WLAN Access System it is connected to or a dedicated TLS server.	O	WLAN-WO-7
WLAN-WO-9	The DO VPN must be administered over a secure connection (i.e., SSH, TLS, DTLS, IPSec).	T=O	
WLAN-WO-10	All Red Compute or EUDs must connect to the DO WLAN through a wired connection (e.g., Ethernet).	T=O	
WLAN-WO-11	The DO WLAN must strip and replace the Data Link Layer protocol headers between the DO WLAN and the Red Compute platform.	T=O	
WLAN-WO-12	The DO WLAN must have one layer of Platform Encryption.	O	

5.3 RETRANSMISSION DEVICE

An RD is a government-owned device dedicated as a passthrough between the Red Compute and the untrusted Black Network. The RD has two important functions, first, to separate out the wireless transport from the Red Compute platform and secondly, to provide a separation point between the Red Compute platform and any untrusted Black Network. An ideal RD can be connected to any type of medium (e.g., Cellular, Wi-Fi, SATCOM, Ethernet) to gain access to the Black Network. The RD, as part of a Composed Hardware-Separated EUD, must be physically connected to the DO Encryptor using a wired connection. There are currently no selector requirements for an RD, but instead an objective requirement to be selected from the CSfC Components List for Traffic Filtering Firewalls. Additionally, there are functional security requirements described within the MA CP. An RD PP is currently in draft, with a release date to be determined.

DRAFT

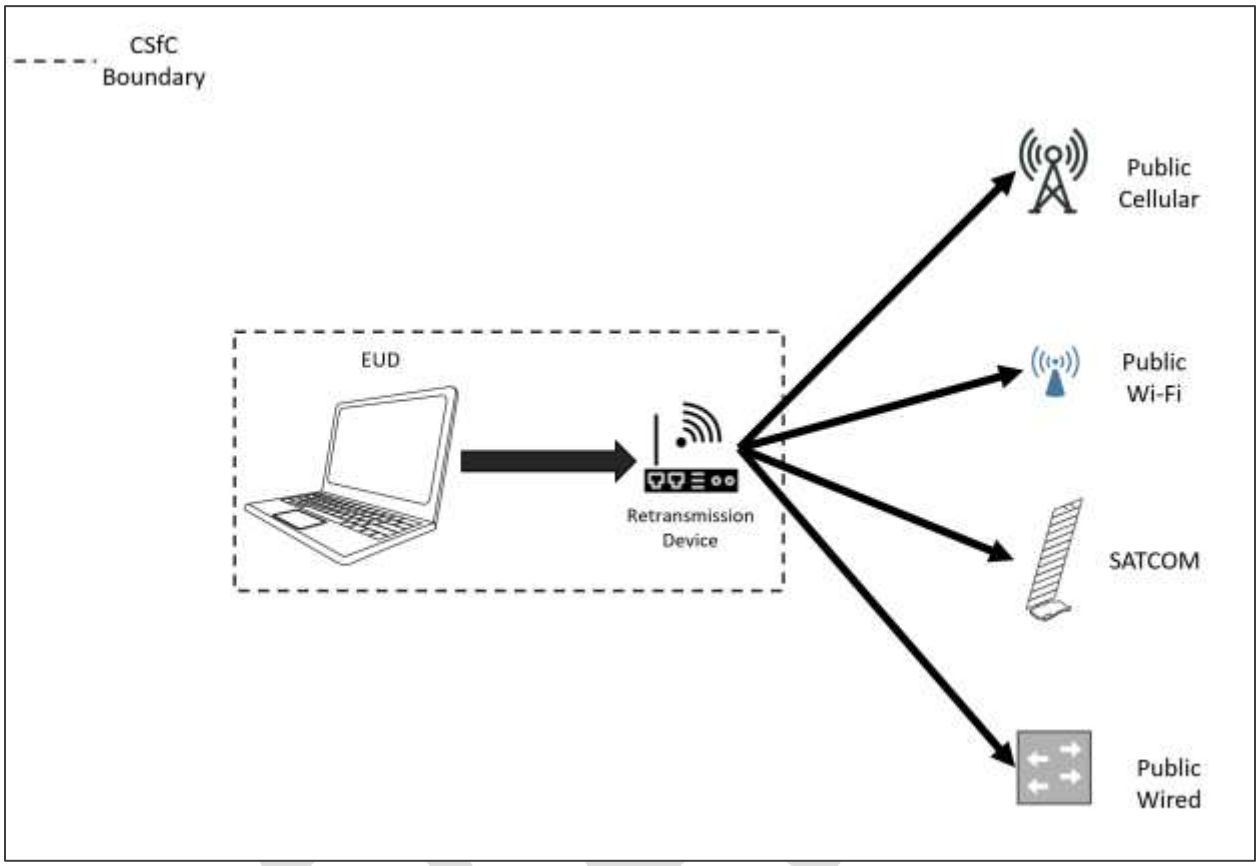


Figure 5. MA CP Retransmission Device

Table 8. RD Requirements

Note: Requirement numbering for this table has been updated from previous versions.

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PS-42	If the solution uses an RD, it must be selected from the RD lists on the CSfC Components List.	All	T=O	
MA-RD-1	An EUD or DO must connect only to RDs.	All	T=O	
MA-RD-2	An RD must provide EUDs with connectivity to the MA Solution infrastructure via any Black Network using Wi-Fi or an Ethernet cable.	All	T=O	
MA-RD-13	The RD must be administered using HTTPS.	All	T=O	MA-RD-31 or MA-RD-32

MA-RD-14	The RD must require authentication of the administrator before any configuration changes can be made. (**Note:** The user may have limited access to configure the EUD without administrative credentials.)	All	T=O	
MA-RD-15	The RD default Administrator credentials must be changed during provisioning.	All	T=O	
MA-RD-16	The RD must be configured to allow the least number of EUDs required for the mission.	All	T=O	
MA-RD-19	The RD must only permit charging on USB ports and interfaces.	All	O	Optional
MA-RD-20	The RD must not permit file sharing.	All	T=O	
MA-RD-21	The RD must require Administrator authentication prior to downloading logs or configuration files.	All	T=O	
MA-RD-22	The RD must only allow firmware updates signed by the RD manufacturer.	All	O	Optional
MA-RD-23	The RD must prevent the ability to boot into recovery mode.	All	O	Optional
MA-RD-24	Withdrawn			
MA-RD-29	If the RD is connected to a Black Network that requires user interaction (e.g., captive portal wireless, 802.1x user authentication), neither the DO nor the Red Compute platform must be used to provide any input.	All	T=O	MA-HS-5 or MA-RD-41 through MA-RD-45
MA-RD-30	Initial provisioning of the RD occurs in a physically secure area.	All	T=O	
MA-RD-31	The RD must be administered using a hard-wired connection.	All	T=O	MA-RD-13 or MA-RD-32 or MA-RD-33
MA-RD-32	The RD must be administered using a wireless connection in a physically secure area.	All	T=O	MA-RD-13 or MA-RD-31 or MA-RD-33
MA-RD-33	The RD must be remotely administered from an enterprise management capability on a Black Network approved by the AO.	All	T=O	MA-RD-31 or MA-RD-32
MA-RD-34	The RD must disable Firmware-Over-the-Air (FOTA) updates from the cellular carrier.	All	O	Optional
MA-RD-35	The RD must have one layer of Platform Encryption.	All	O	Optional

DRAFT

MA-RD-36	The RD must connect to the EUD/DO VPN using a hard-wired connection (i.e., Ethernet or Ethernet over USB).	All	T=O	MA-RD-37
MA-RD-37	The RD must connect to the EUD VPN using a wireless connection with the appropriate virtual isolation, as detailed in the VZ Table	WC, VZ	T=O	MA-RD-36
MA-RD-38	The RD must block all outgoing traffic from the EUD/DO VPN that is not required to connect to the Outer VPN Gateway (i.e. Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), Domain Name Server (DNS)).	All	T=O	
MA-RD-39	The RD must block unauthorized incoming traffic to the EUD/DO VPN.	All	T=O	
MA-RD-40	The baseband processor providing connectivity on the Black Network must be physically separate from the main processor.	All	O	

5.4 SINGLE FORM FACTOR HARDWARE-SEPARATED EUDS

With the increased emphasis on Hardware-Separation within the CSfC CPs, between the Red Compute, DOs, and RDs, there is an option to combine all hardware components into a single form-factor device to improve user experience.

An important aspect of a single form factor Hardware-Separated device is how it is managed. There are generally four accepted ways to configure and manage such a device:

- Have three separate dedicated management interfaces for the Red Compute, DO, and RD
- Implement a physical KVM into the platform
- Manage each component via enterprise management features
- Manage through a Virtualized EUD via a controlled interface (See Section 6)

5.4.1 KVM CONTROL OF THE SINGLE FORM FACTOR

The KVM establishes a physically and electronically isolated bus between the Red Compute platform, DO, and RD. The KVM control line initiates physical switching between the Red Compute platform and RD interfaces for management capability. The KVM data line provides the data path for multiplexing the display and/or keyboard in support of local management functions of the Red Compute platform and RD.

The Red Compute platform must not have any interaction with captive portal wireless or 802.1X user authentication. A KVM greatly reduces risk by isolating the Red Compute platform, adding an additional attack path an adversary must overcome. Composed Hardware-Separated EUDs must employ a solution

DRAFT

that allows interaction with any captive portal or 802.1X user authentication to be administered on the RD itself.

Table 9. Hardware-Separated Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-HS-1	The Red Compute platform hardware components must maintain physical, electrical, and logical separation from the DO Encryptor and RD. Sharing of CPU, memory, storage, cryptographic components, or ancillary components between hardware platforms **is not** permitted.	HS	T=O	
MA-HS-2	The DO hardware components must be physically separated from the Red Compute platform and the RD. Sharing CPU, memory, storage, cryptographic components, or ancillary components **is not** permitted.	HS	T=O	
MA-HS-3	The RD must be physically separated from the EUD and DO. Sharing of CPU, memory, storage, cryptographic components, or ancillary components **is not** permitted).	HS	T=O	
MA-HS-4	If using a Composed Hardware-Separated EUD, the EUD must implement a KVM capability that enables the user interface switching between the Red Compute platform and the RD.	HS	O	
MA-HS-5	If using a KVM, the KVM must be NIAP validated.	HS	T=O	

5.5 Deployment Options for Hardware-Separated EUDs

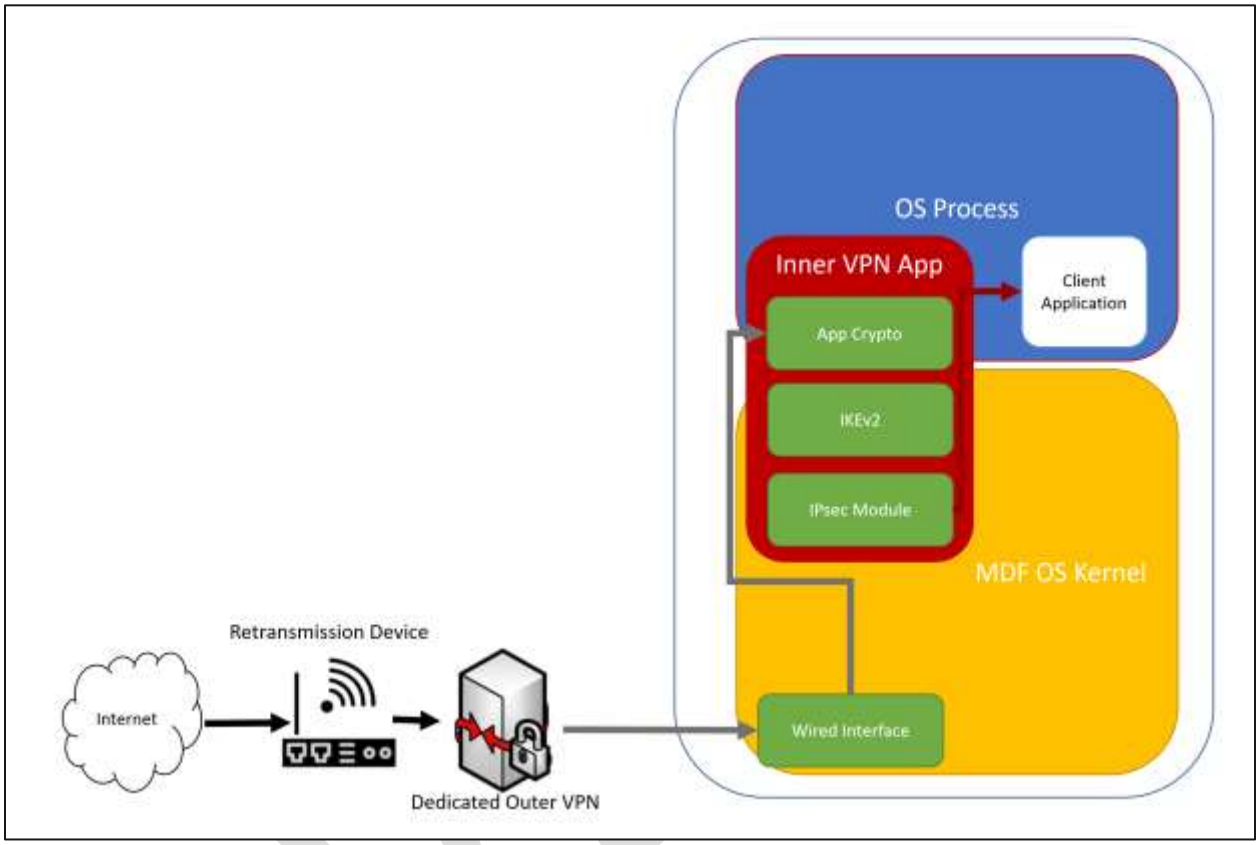
The following section restates the high-level deployment options for the Hardware-Separated EUD for MA and CWLAN CPs.

5.5.1 Mobile Device Fundamentals Hardware-Separated EUDs

When an MDF EUD is used as the Red Compute for an MA Solution, the MDF EUD must use a hardwire connection to the DO. To preserve the mobile nature of the MDF EUD, an RD must be used, or the DO must use a wired connection to the Black Network. It is also recommended that the EUD form factor integrate into a sleeve or case with an MDF EUD directly attached. Additional SWaP requirements should be considered, as this device will contain three separate computing platforms. The RD and DO must be managed either locally via a wired interface or remotely as detailed in Section 5.2.3.

DRAFT

459



460

461 **Figure 6. MA MDF Hardware-Separated EUD**

DRAFT

462

463 **Figure 7. Proposed MA MDF Case with Hardware-Separated RD**

464 The MDF EUD must use a hardwire connection to the DO when an MDF EUD is used as a Red Compute
465 for a CWLAN Solution. Furthermore, it is recommended that the EUD form factor incorporate a sleeve
466 or case that allows an MDF EUD to be directly attached. Additional SWaP requirements should be
467 considered, as this device will contain two separate computing platforms. The DO must be managed
468 either locally via a wired interface or remotely, as detailed in Section 5.2.3.

469

DRAFT

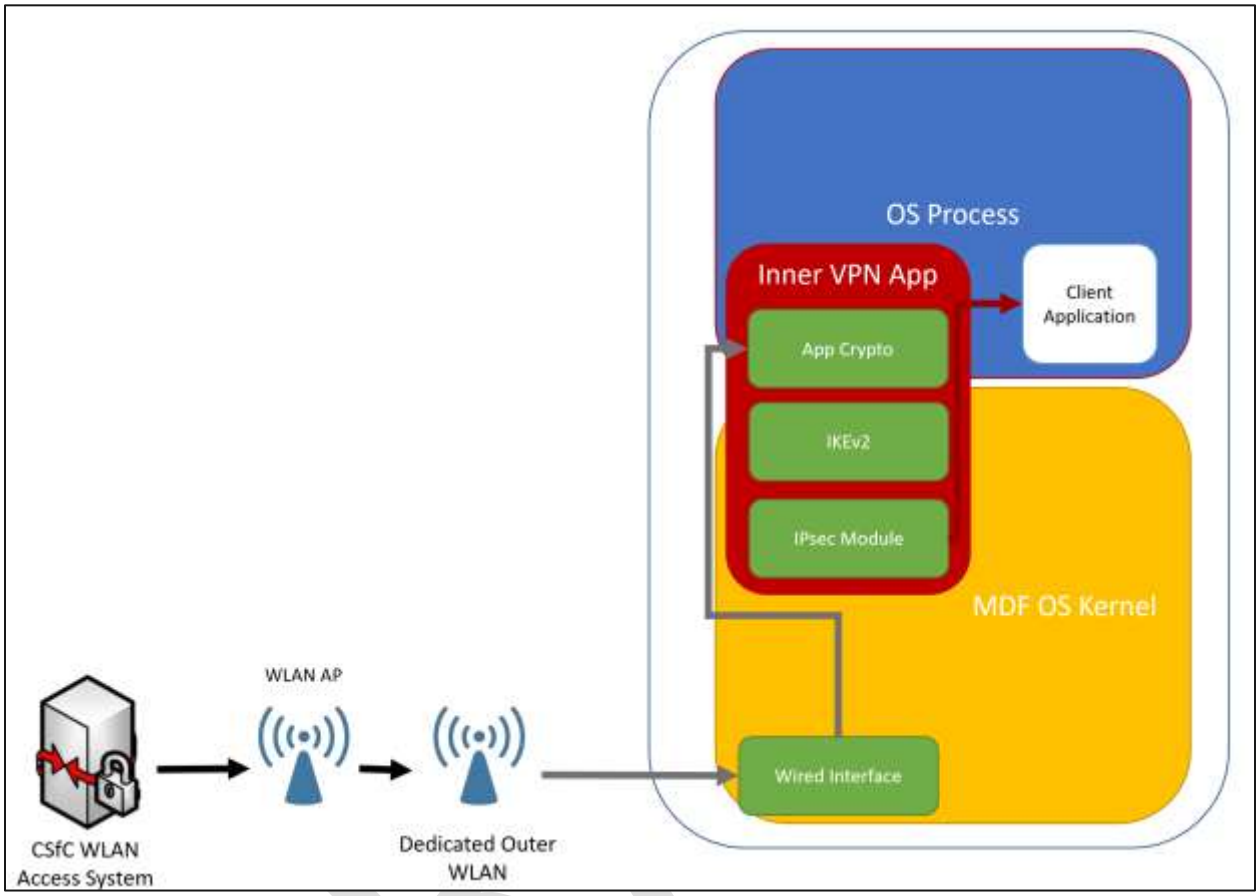


Figure 8. CWLAN MDF Hardware-Separated EUD

5.5.2 COMPOSED HARDWARE-SEPARATED EUDS

If a Composed EUD is used as the Red Compute for an MA solution, the Composed EUD must use a hardwire connection to the DO. The ideal form factor for a laptop-like system is for both the DO and RD to be placed within the system chassis to minimize complexity and user impact. Additional single form factor applications are described in Section 5.4. The RD and DO must be managed either locally via a wired interface or remotely, as detailed in Section 5.2.3.

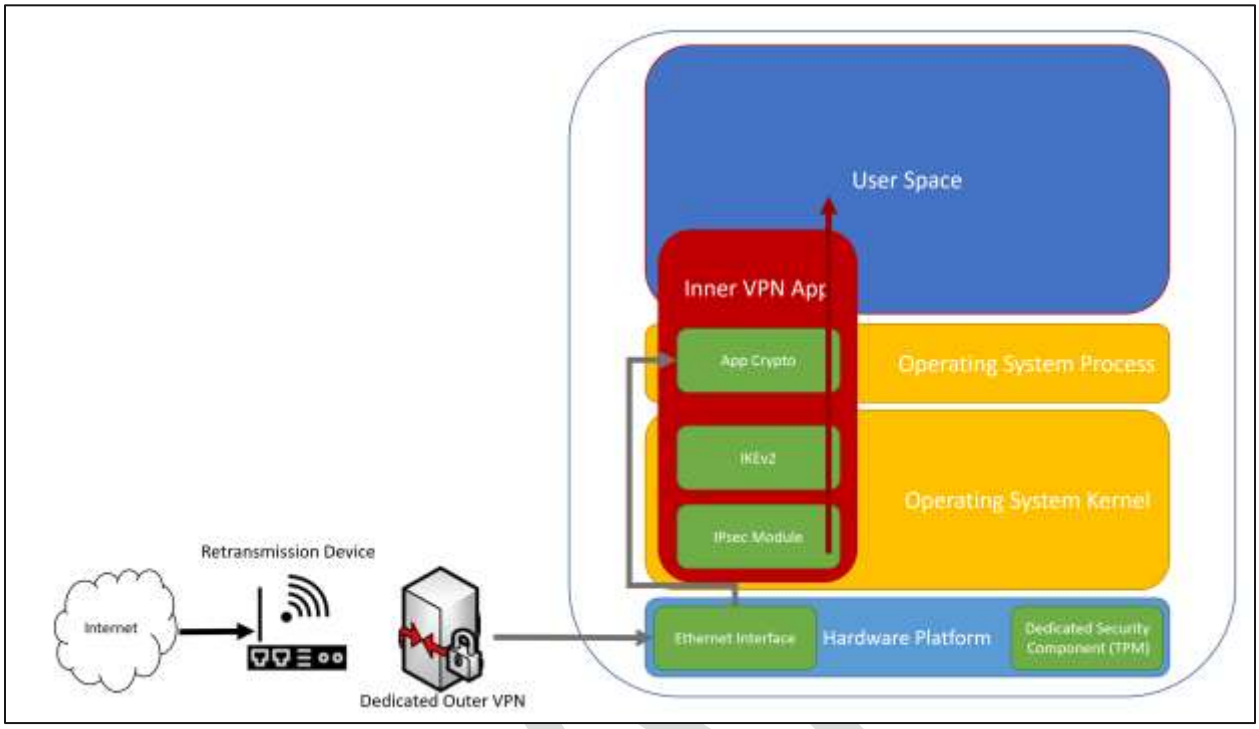


Figure 9. MA Composed Hardware-Separated EUD

If a Composed EUD is used as the Red Compute for a CWLAN solution, the Composed EUD must use a hardwire connection to the DO. The ideal form factor for a laptop-like system is for the DO to be placed within the system chassis to minimize complexity and user impact. Additional single form factor applications are described in Section 5.4. The DO must be managed either locally via a wired interface or remotely as detailed in Section 5.2.3.

5.6 HARDWARE-SEPARATED EUD'S WIRED CONNECTION TO BLACK TRANSPORT

For MA CP, the RD is intended to handle high risk functions, especially wireless connectivity. If wireless connectivity is not required for the EUD's Black Transport, an RD is not required, and the DO VPN may be physically connected to the Black Network. This applies to all form factors of MA CP Hardware-Separated EUDs.

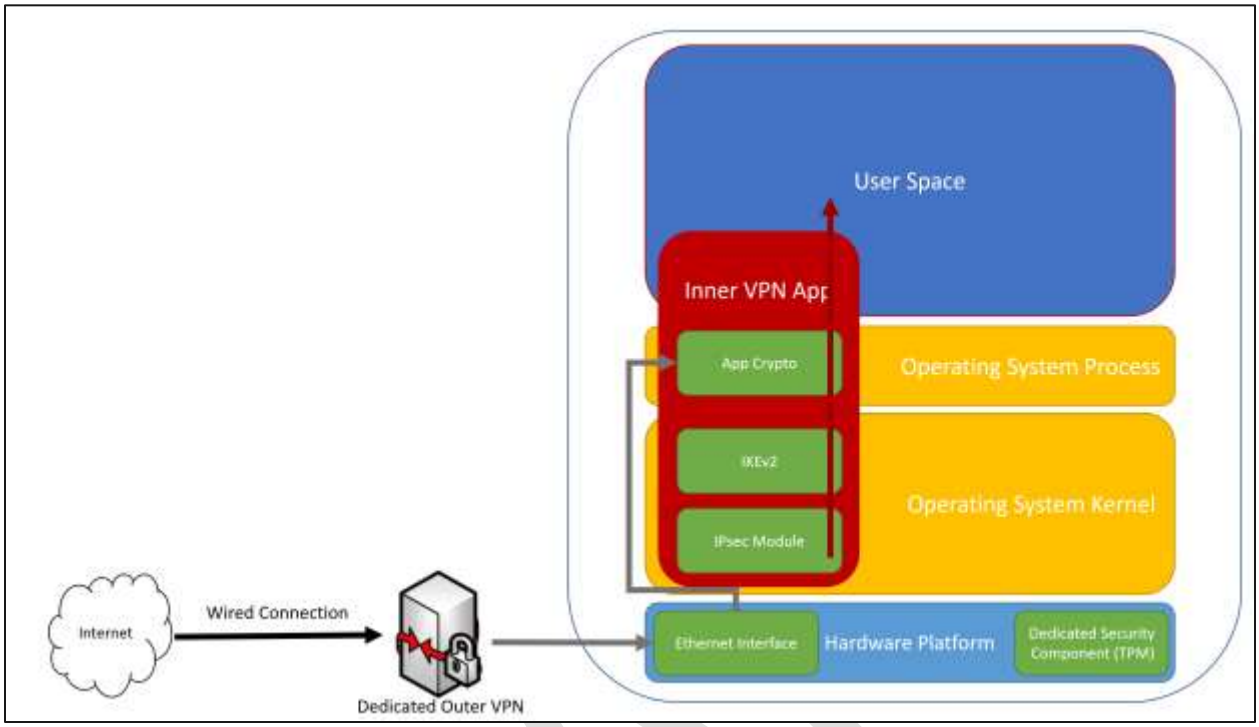


Figure 10. MA Composed Hardware-Separated EUD with no RD

5.7 VIRTUALIZED HARDWARE-SEPARATED EUDS

The Virtual EUD concept can also be used independently of the Virtual Machine (VM) interaction with the RD and the Wi-Fi driver isolation to further improve EUD security. Combining both the Virtual EUD and the DO concepts increases the security of the EUD.

When a Virtual EUD is used as the Red Compute for an MA Solution, the Virtual EUD must comply with all virtualization requirements. The Inner VPN Client must reside within in its own virtual instance, and the Red Compute must be connected to the DO through a hardwire connection. For a laptop-like system, the ideal form factor is for the DO and RD to be placed within the system chassis to minimize complexity and user impact. Additional single form factor considerations are described in Section 5.4. The DO and RD must be managed either locally via a wired interface or remotely, as detailed in Section 5.2.3.

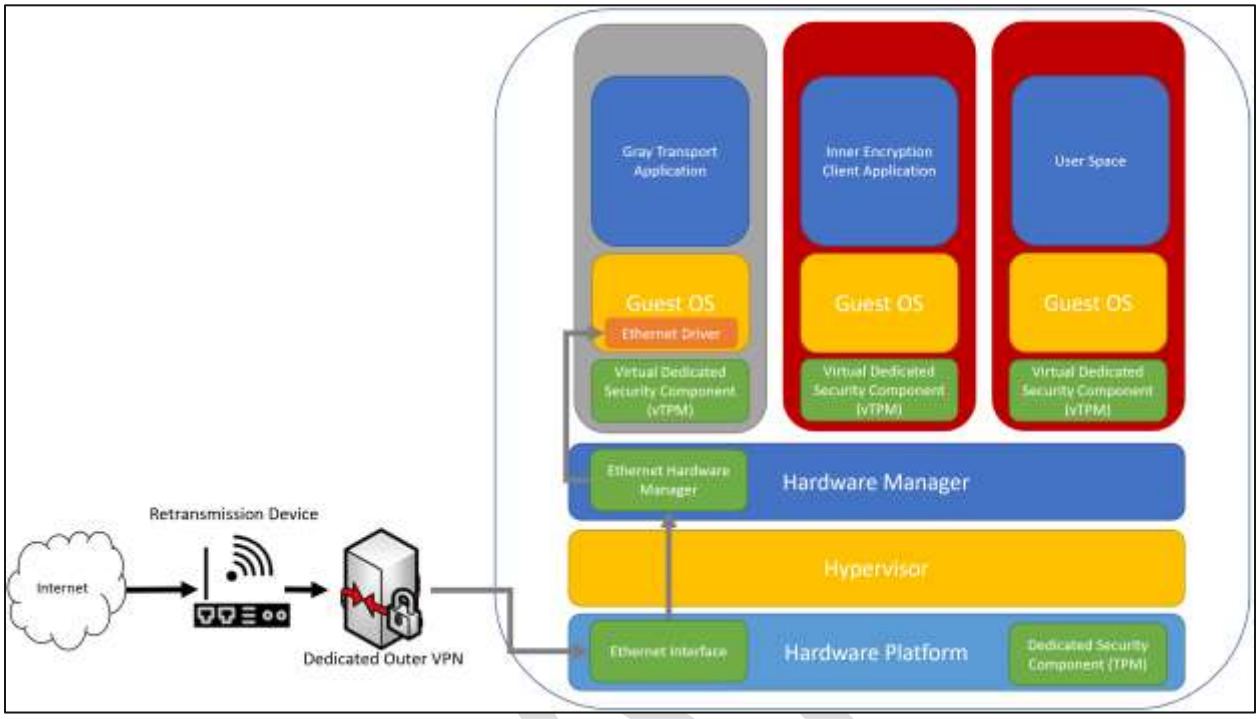


Figure 11. MA Virtual Hardware-Separated EUD

When a Virtual EUD is used as the Red Compute for a WLAN Solution, the Virtual EUD must comply with all virtualization requirements. This includes the requirement that the Inner VPN Client must reside within its own virtual instance and that the Red Compute must connect to the DO through a hardwire connection. For a laptop-like system, the ideal form factor is for the DO to be placed within the system chassis to minimize complexity and user impact. Additional single form factor considerations are described in Section 5.4. The DO must be managed either locally via a wired interface or remotely, as detailed in Section 5.2.3.

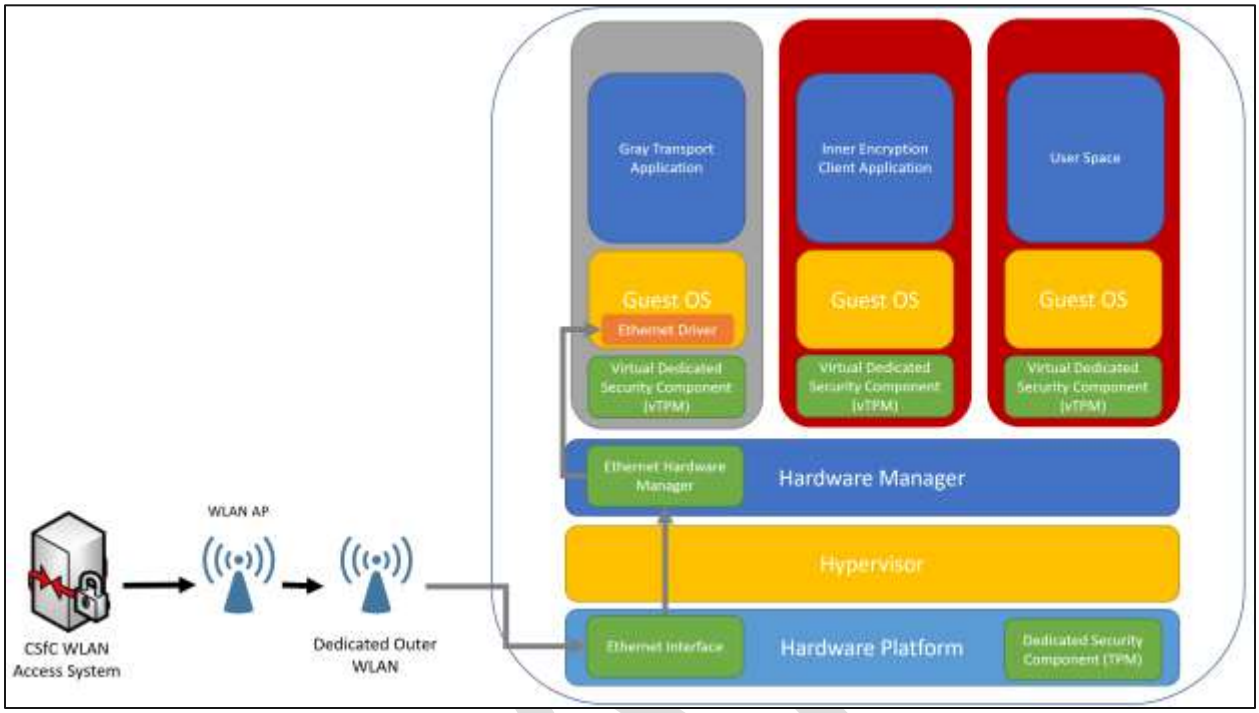


Figure 12. CWLAN Virtual Hardware-Separated EUD

5.7.1 VIRTUALIZED DEDICATED OUTERS

A DO may rely on Virtualization technologies as a Virtualized EUD. In this case, the Virtual DO must either run a VM with an IPSec VPN Client or VPN Gateway from the CSfC Components List. The virtualized DO must comply with all other DO requirements, as detailed within Section 5.2.

DRAFT

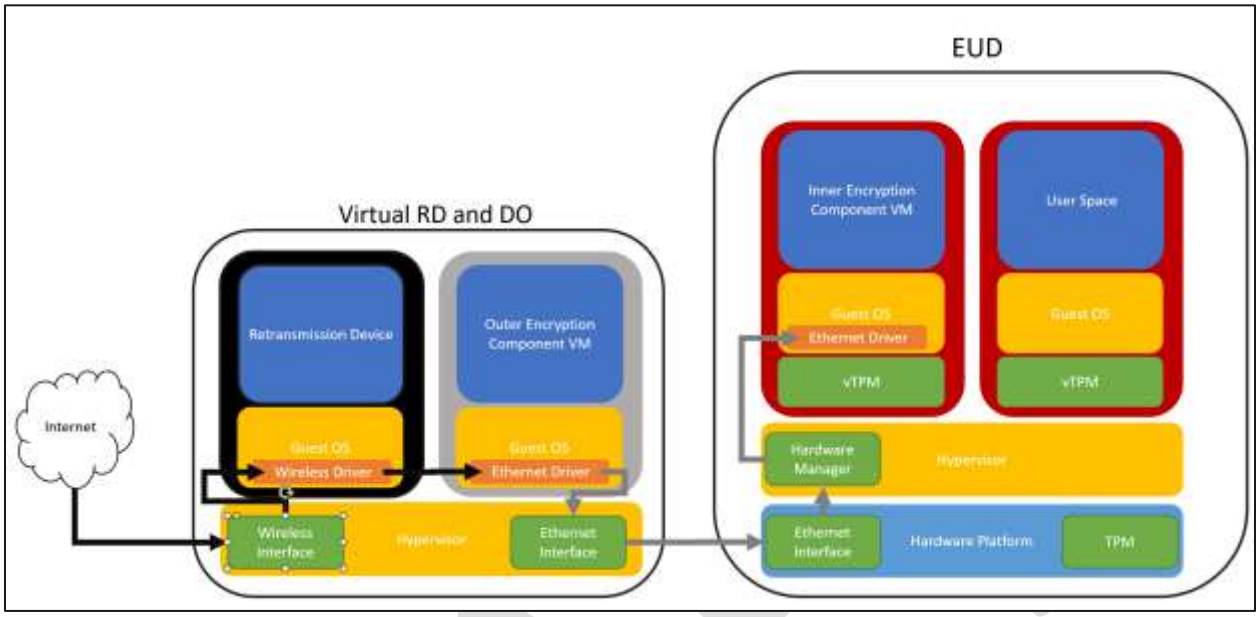


Figure 13. Virtual DO with a Virtualized RD

Beyond hardware reduction purposes, it may be desirable to run an RD and DO on the same hardware platform. In this case, the hypervisor that the DO operates on must be listed on the CSfC Components List. The VM that operates the DO functionality must run an IPsec VPN Client or VPN Gateway. The VM running the RD functionality must be a listed OS or Traffic Filtering Firewall on the CSfC Components list. This concept operates similarly to a Virtualized EUD, with the exception that the platform does not contain any Red applications, such as the Inner Encryption Component or user VM. Therefore, the platform will not contain any Red Data.; however, all other Virtualized EUD requirements apply to the device. As detailed in Section 6.1, this Virtualized DO with a virtualized RD must include the following features to provide separation between the RD VM and DO VM:

- VM Interconnectivity
- Limited VMs
- Read Only VMs
- VM Signature Validation
- Processor Pinning/Isolation
- Memory Isolation
- Encrypted Memory
- Hardware Passthrough

One important feature of hardware isolation permits the assignment of dedicated network interfaces to the RD VM and DO VM for driver abstraction purposes. The RD VM must be assigned the internet-facing network interface so that it can run the driver for that interface within the RD VM, whether the interface

is Ethernet, Wi-Fi, cellular, or another network interface type. The DO VM will be assigned the wired interface that is directly connected to the EUD.

A benefit of this solution is the increased control over the RD through components such as the Read Only VM, VM restriction, and VM signature validation. When these are applied to the RD VM, changes to, and the capabilities of, the RD are significantly limited and temporary in nature. Additionally, combining this solution with validating the signature or hash of the RD VM provides assurance that the RD will remain in a known good state.

This Virtualized DO with RD Virtualization may be combined with RD Control, as detailed in Section 6.2, to enable a virtualized EUD to interact with the virtual RD through a controlled application for RD configuration. During this interaction, the Encryption VMs and user VMs associated with the EUD and DO must be disabled, allowing only the dedicated VMs to run the RD interaction. Once the interaction is complete, the Interaction VMs must be disabled, and the RD VM itself must be restarted before normal VM operations can be conducted.

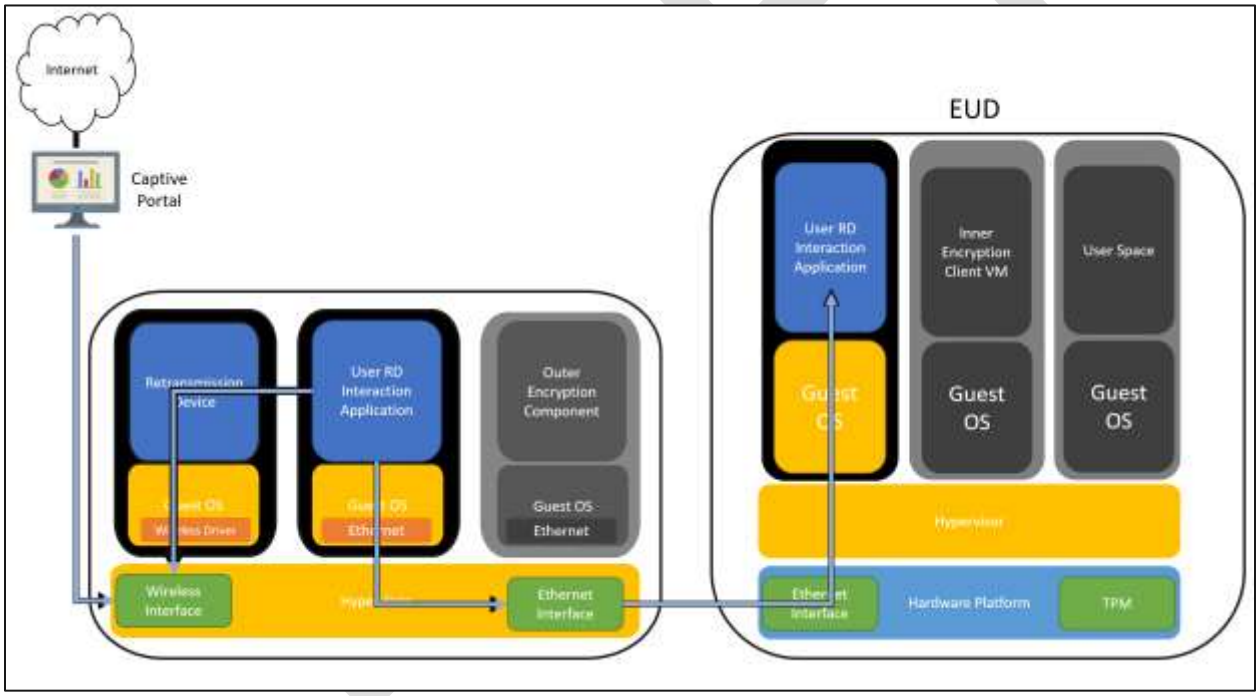


Figure 14. Virtualized EUD with Virtualized DO and RD for Captive Portal Interaction

5.7.2 Virtualized Dedicated Inner and Outer

Within the Hardware-Separated EUD concept, included are both the DO, the Dedicated Inner, and Red Compute. A Dedicated Inner is an option in cases when the Red Compute Hardware cannot perform encryption and cannot satisfy CSfC Program encryption requirements, or when a customer desires encryption to occur off the EUD platform. The Dedicated Inner is, for all intents and purposes, a DO

functioning as the inner layer of encryption of a CSfC solution and requires a DO to operate. The preferred method is for the Dedicated Inner and Outer to be Hardware-Separated components, but allowing the Dedicated Inner to be contained within the same physical component. If an RD is required, the RD must remain its own separate hardware component. Virtualization can further enhance the security of the Dedicated Inner and Outer by allowing a single hardware platform to house both the Inner and Outer Encryption Components for an EUD. In this case, the Virtual Dedicated Inner and Outer VMs must separately run either a VM with a listed IPSec VPN Client or VPN Gateway. The virtualized Dedicated Inner and Outer must meet all other DO requirements, as detailed in Section 5.2.

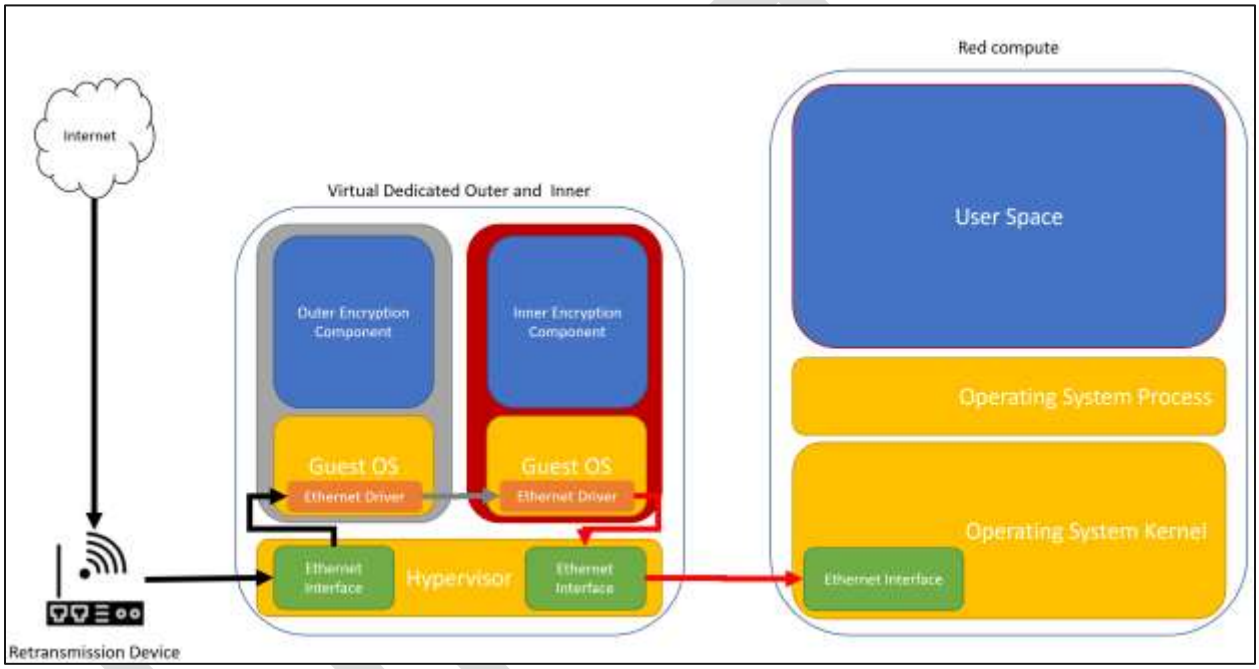


Figure 15. Virtualized Dedicated Inner and Outer

6 MANAGING RETRANSMISSION DEVICES THROUGH A VIRTUALIZED EUD

To control the RD or DO, use of a Virtualized EUD is required in combination with a controlled interface to provide direct control and interactions of either the DO or RD. This approach enables solutions relying on Virtualized EUDs the option to interact with any captive portal or 802.1X user authentication, as well as administer the RD or the DO. The captive portal interaction itself must be conducted by the RD while the EUD controlling the RD performs the interaction from an isolated virtual domain dedicated to this interaction. For more information, see Section 6.2.

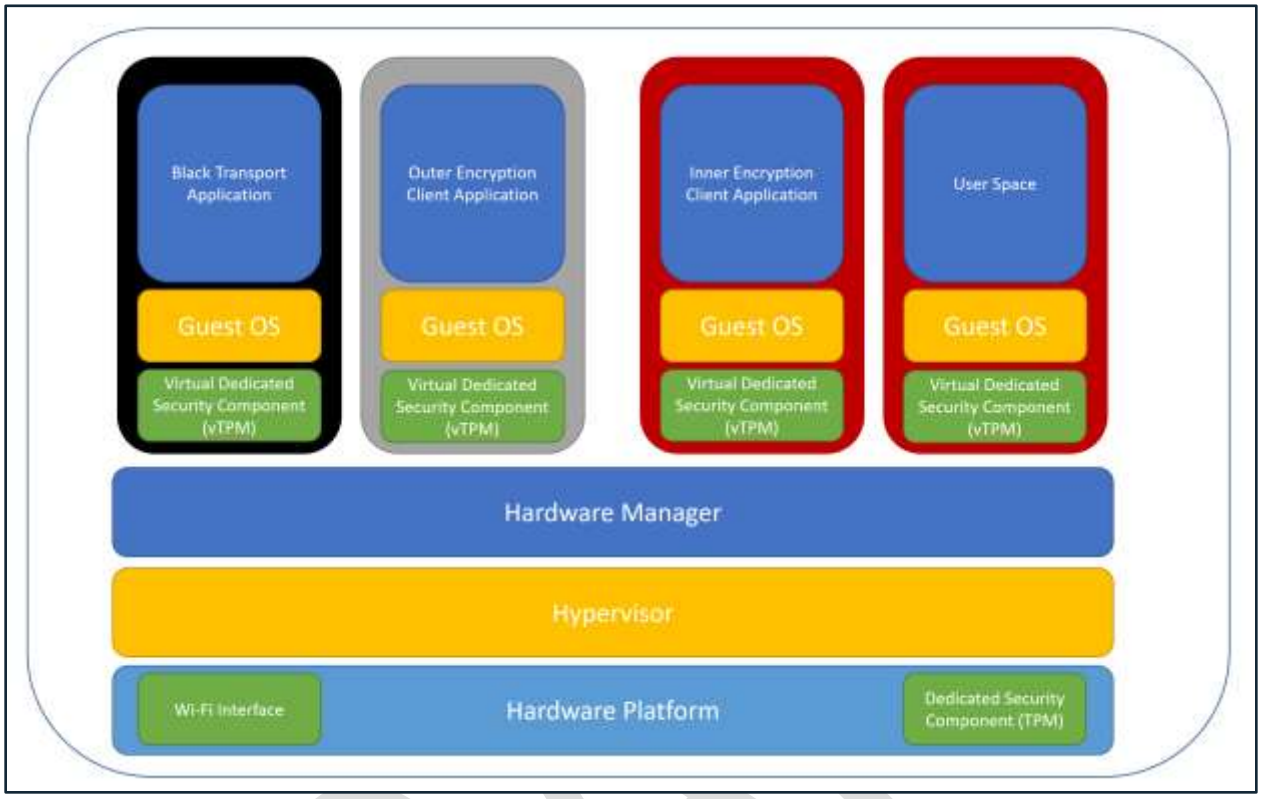


Figure 16. Virtualized EUD in MA

Within the MA CP, the Virtualized EUD enhances the security of a normal Composed or MDF EUD by isolating the encryption clients into separate VMs, as well as the network stack and user space, into their own VMs. This is accomplished through a Type 1 hypervisor, which provides additional security for the component by isolating the storage, driver, memory, and processing into separate virtual instances.

For a Virtualized EUD, the hypervisor replaces the OS and runs directly on the EUD Hardware Platform. Virtualized EUDs create virtual instances that contain both kernels and OSs that are used to create isolated domains. Applications and EUD functions, such as IPsec Client, WLAN Client, or TLS Client, are placed into separate namespaces within their own isolated virtualized environments with little to no resource sharing between the virtual environments.

These isolated domains allow multiple EUD components to be securely implemented into a single piece of hardware while ensuring a separate IP stack is used for each connection layer. The hypervisor provides the virtual networks used by the domains for internal network connections that are required for dual layers of encryption. The standard MA CP EUD should include the following sub-domains:

1) a user domain where the user can interact with the EUD

2) a transport domain to connect to the Black Transport Network

3) a transport domain to connect to the Outer Encryption Component

4) a transport domain to connect to the Inner VPN Gateway

End users should only have access to End User domains, while all other domains should be restricted to an administrator. Additional domains may be added to support device management functions.

6.1 HYPERVISOR ARCHITECTURE

To use a Virtual EUD to control and interact with the RD, the following features must be enabled:

- VM Interconnectivity
- Limited VMs
- Read Only VMs
- VM Signature Validation
- Processor Pinning/Isolation
- Memory Isolation
- Encrypted Memory
- Hardware Passthrough

The separation that the Type 1 hypervisor provides between the VMs must be considered when establishing interconnection between VMs to support the flow of data from the Black untrusted network to the Red user space. Each VM should have limited connection to only the necessary core functions required for VM functionality for their given application. Most hypervisors have virtualized switching technology that can be used to allow routing between the VMs and even the hypervisor. These virtual switches should be separated based on the data type they handle, such as Black, Gray, and Red. For example, there should be a separate virtual switch to handle the Black data, Gray data, and Red data, and a dedicated switch to pass data between the Black Network and the Black VM. Figure 12 illustrates Virtual EUDs using separate virtual switches, enabling communication between the VMs, with each switch dedicated to the specific data type transiting the switch.

DRAFT

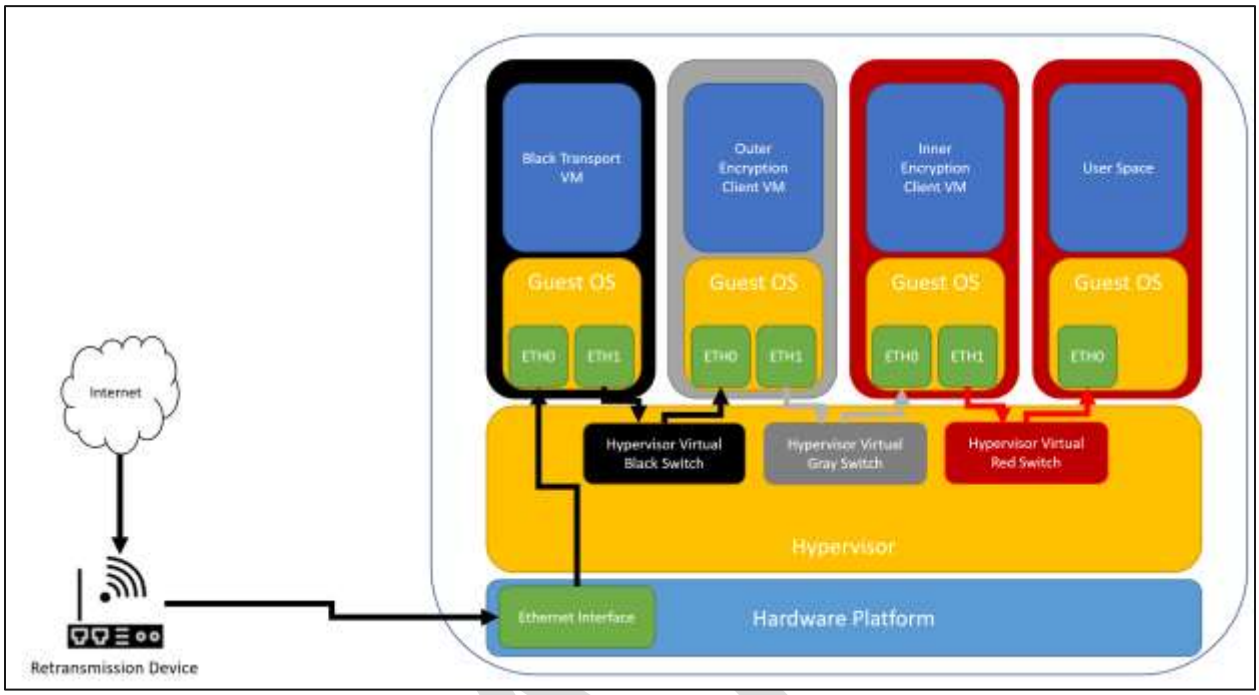


Figure 17. VM Interconnectivity

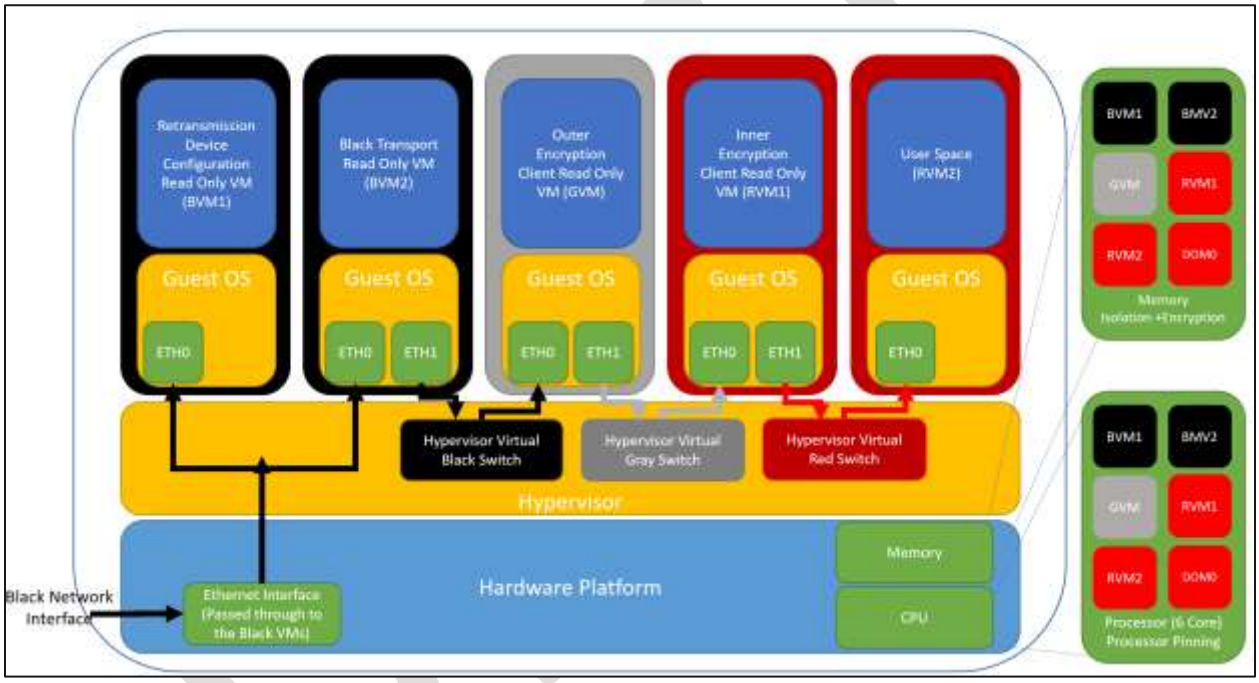
Another function that can be leveraged is running an independent firewall within each guest VM. This limits what the VM can send and receive on its own interfaces and adds an additional layer of network security to the EUD.

VMs within a Virtual EUD should be limited to only the necessary core functions required for operation and all other additional functionality should be removed. For example, the Outer Encryption VM should include only the outer encryption client, network supplicants, firewall, and any additional supporting libraries. It should not contain any non-essential functionality. Non-essential functionality may include user applications, text editors, and even user interfaces. These limited functionality principals should be applied to all VMs within a Virtual EUD to further reduce the attack surface that each VM presents to the Virtual EUD.

Within virtualization technology is the concept of 'read only' VMs, in which the virtualized guest OS file system is in a 'read only' state. In this state, no changes made to the guest OS's file system are permanent nor do they persist after rebooting the VMs. This guarantees the VMs will always boot into a known good state, and any errors that occur within the VM are not persistent on reboot. These traits are particularly beneficial for VMs that provide network functionality of the EUD to prevent modifications to the file system and reduce persistence through reboots. The User Space VM is not required to operate as read only; all other VMs are required to be set to read only.

649 Building Read Only VMs relies on VM signature validation, which is the process of attestation by the
650 hypervisor performing health and integrity checks on the Read Only VMs image to ensure it has not
651 been altered or changed. The hypervisor must verify the health and integrity of each bootable VM to
652 confirm no changes have been made.

653 Processor Pinning/Isolation reserves CPU cores for VMs, preventing the host OS from using them,
654 ensuring dedicated resources and consistent performance. Each VM Domain should have a dedicated
655 processor pinned to the VM. In addition, the CPU register contents should be either encrypted or
656 deleted when a VM stops running. To prevent the leakage of information in CPU registers to
657 components such as the hypervisor, each VM in a Virtual EUD must implement Processor
658 Pinning/Isolation, giving each VM its own dedicated Processor.



659

660 **Figure 18. Virtualized EUD with Virtual Isolation Features**

661 Memory Isolation gives each VM dedicated memory, ensuring there is no shared memory between VMs
662 and the hypervisor itself. Secure memory encryption enables the VMs and hypervisor to work together
663 to encrypt portions of a VM's memory and page files using a unique key, preventing sensitive data
664 leakage in the VM memory and preventing hypervisor-based attacks. All VMs must have separate
665 memory dedicated to that VM.

666 Hardware Passthrough occurs when the hypervisor grants a VM direct access and control over the
667 physical hardware of the compute platform. Traditionally, this is accomplished through Peripheral
668 Component Interconnect (PCI) Passthrough, which allows control of physical devices to be assigned to

guests. PCI Passthrough enables the assignment of a PCI device (e.g., NIC, disk controller, HBA, USB controller, firewire controller, soundcard, etc.) to a VM guest, giving it full and direct access to the PCI device. Within CSfC, this approach has been used to pass the Wi-Fi network interface directly to the VM instead of the hypervisor. In this architecture, the Ethernet network interface must be passed to the Black VM.

6.2 Virtual Machine Interaction with a Retransmission Device

The capability to control the RD is meant to either allow the End User to configure network connectivity in the field or interact with a service such as a captive portal. For captive portal interactions, it is still preferred to use a physically separate device or to have the RD manage the entire captive portal interaction itself, although this may not be possible in all use cases.

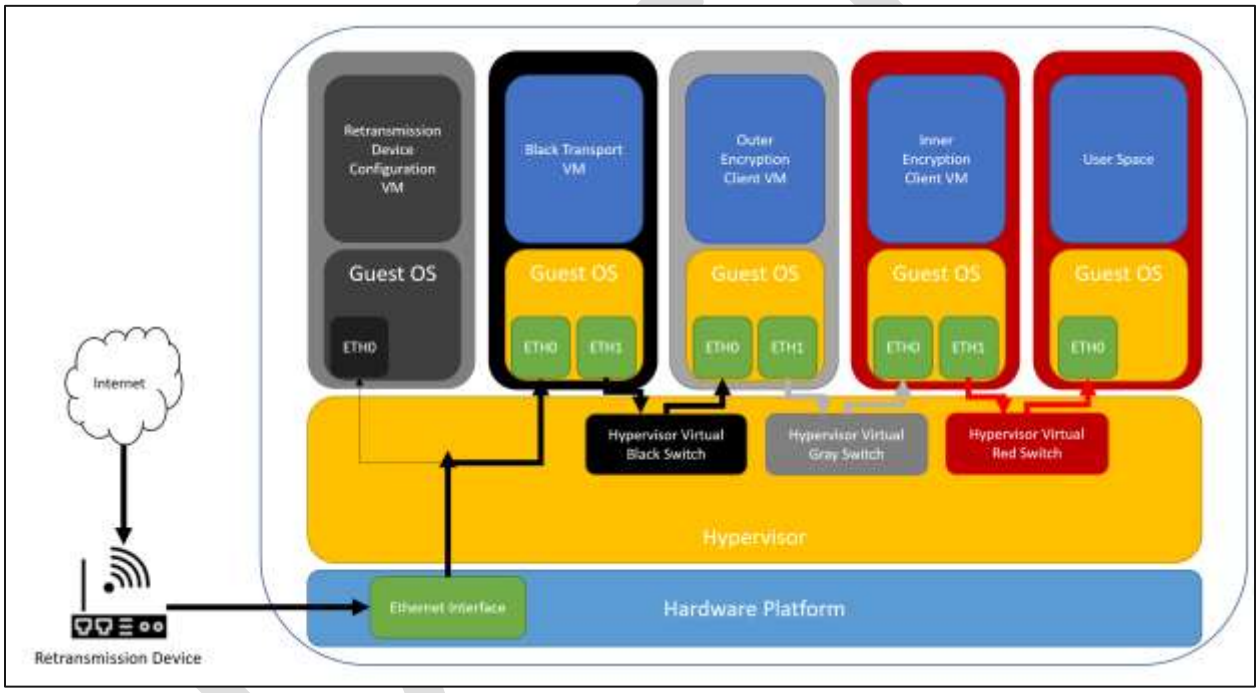


Figure 19. Virtual EUD RD Control Normal Operation

Figure 19 illustrates a Virtualized EUD during normal operations, including the virtualization and the nested VPN tunnels connected to the VPN gateways in order to connect to the CSfC Solution. Within this architecture, a VM must be dedicated to interacting with the RD, as it cannot perform any other functions. During normal EUD operations, the VM must be powered off, as shown in Figure 19. If interaction with the RD or a captive portal is required, as shown in Figure 20, the VMs used for the CSfC connection must be shut down, and the dedicated VM should be activated to grant the user access to its interface, solely for the purpose of interacting with the RD. The VM is a limited VM that remains

powered off, unless in operation, and should automatically shut down once its required operation is completed.

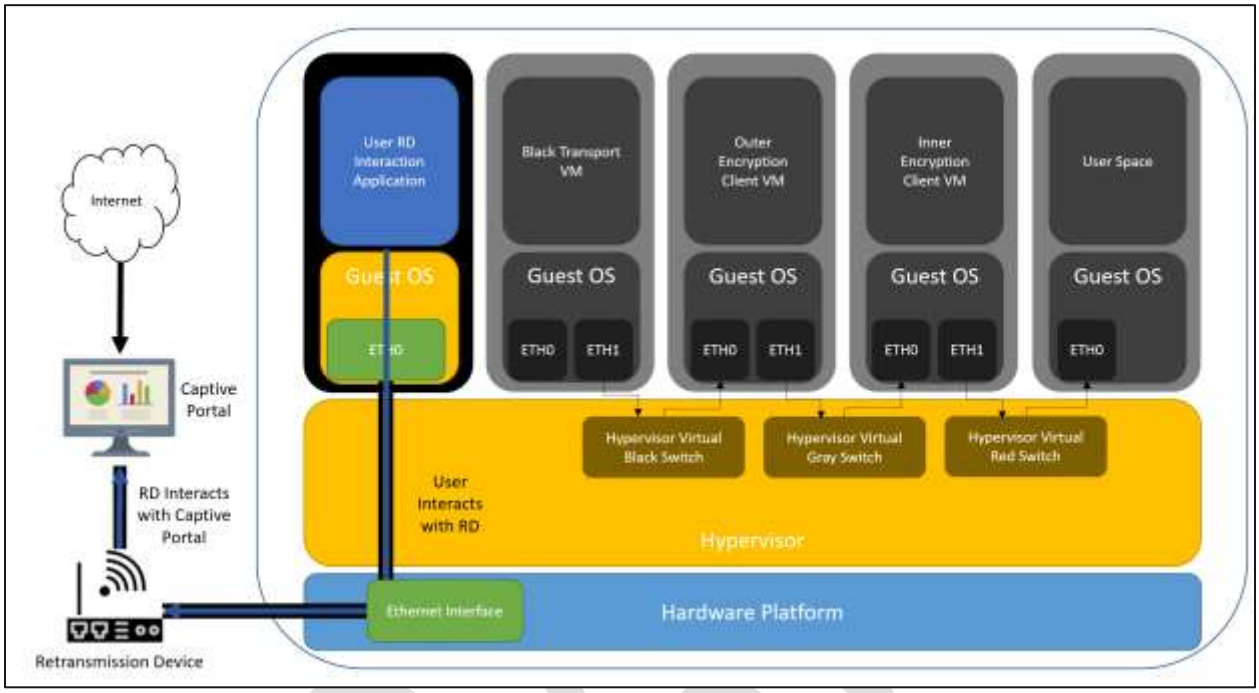


Figure 20. Virtualized EUD for Captive Portal Interaction

As shown in Figure 20, when the user is required to interact with a captive portal, the dedicated VM interacts directly with the RD though a controlled interface, such as VNC, SSH X11 or similar such protocols, to enable a GUI on the RD to allow user interaction. The user will then use the RD's GUI interface to directly interact with the captive portal to accept terms and enter information required for internet connectivity. Once this action is completed and the connection to the internet has been established, the VM should shut down, and the hypervisor will start the CSfC DiT VMs.

The following are the requirements which will be added to the MA CP Virtualization Requirements and Hardware Separation tables for the purpose of interacting with an RD and a DO.

Table 10. Virtualization for RD & DO Interaction Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-VZ-25	In a Virtualized EUD, all VMs, except the User VM, must be a Read Only VM.	VZ	T=O	
MA-VZ-26	In a Virtualized EUD, the hypervisor must validate the health and integrity of each bootable VM to confirm it has not been changed. If a change has	VZ	T=O	

	been detected, the VM must not be allowed to boot.			
MA-VZ-27	In a Virtualized EUD, all VMs must have their own dedicated memory exclusive to that VM.	VZ	T=O	
MA-VZ-28	In a Virtualized EUD, all VMs dedicated memory must enable VM memory encryption.	VZ	T=O	
MA-VZ-29	In a Virtualized EUD, the Ethernet network interface must be passed to the relevant Black Transport VM.	VZ	T=O	
MA-VZ-30	In a Virtualized EUD, each VM must implement Processor Pinning/Isolation providing each VM with its own dedicated Processor.	VZ	T=O	
MA-RD-41	The RD must be managed over a dedicated wired interface.	VZ	T=O	MA-RD-29 Or MA-HS-5
MA-RD-42	When using a Virtualized EUD to interact with the RD, the VM dedicated to the RD interaction must not be the same VM as the as the Black Transport VM.	VZ	T=O	MA-RD-29 Or MA-HS-5
MA-RD-43	When using a virtualized EUD to interact with the RD, the VM dedicated to the RD interaction must not interact directly with a captive portal or other such service. The RD must manage this interaction.	VZ	T=O	MA-RD-29 Or MA-HS-5
MA-RD-44	When using a virtualized EUD to interact with the RD, the interaction between the RD and VM dedicated to the RD interaction must occur through an NSA-approved, secure controlled connection.	VZ	T=O	MA-RD-29 Or MA-HS-5
MA-RD-45	When using a virtualized EUD to interact with the RD, the VM dedicated to the RD interaction must automatically shut down once the required operation is completed or within a timeframe under 5 minutes.	VZ	T=O	MA-RD-29 Or MA-HS-5

7 EUD PROVISIONING

This section extends the provisioning requirements found within the CWLAN to MA CP and DAR CP.

7.1 DATA AT REST EUD PROVISIONING

Provisioning is the process through which EUDs are initialized before first use. During the provisioning process, the Security Administrator (SA) loads and configures the DAR components for the EUD. Initial provisioning of the EUD can be performed on the EUD itself, or use a standalone management system which is physically protected at the same classification level as the EUD. Provisioning is inherently an out-of-band process requiring physical access to the EUD and must be conducted over a wired interface, through a standalone configuration system, or through another CSfC solution provisioning capability. Provisioning includes assigning Government identifiers to the device, installing required applications,

DRAFT

configuring the device's policy and settings, and loading certificates and keying material. Prior to provisioning devices, configuration profiles are created and required device applications are obtained.

Initial provisioning (for all device types) should include the following, in no specific order:

- **Device registration**. Collect identifying information from the EUD, assign Government device identifiers, and update data stores (directory, inventory, and/or authorization) to include the new EUD.
- **Settings configuration**. Load the configuration (within the limitations supported by each device type) that implements policies on allowed and disallowed services (such as wireless) and user authentication parameters (i.e., password length and when to lock the device). Provide the device with other required settings, such as network parameters.
- **Application installation**. Load required applications, including full drive encryption, file encryption, platform encryption, and any other required applications to be loaded during initial provisioning. If possible, unneeded applications should be removed from the device.

Once the EUD is properly configured, certificates/keying material are in place, user login is established, and the user is associated with the device in the registration data, the EUD is ready to be issued to a user. The device is considered classified once it is connected to a classified network or loaded with classified data.

The DAR solution cannot be applied to an EUD that already has stored data. EUD re-provisioning or reuse of DAR components is permitted as long as it is performed in accordance with this CP. If re-provisioning, the EUD must be at the same or higher classification level of previously unencrypted data stored on the approved DAR solution. Prior to re-provisioning an EUD, old data should be removed via cryptographic erase or media zeroization. Media zeroization is the process of fully overwriting the drive. Re-provisioning EUD components from any non-CSfC solution is prohibited.

Table 11. DAR CP EUD Provisioning Requirements (PR)

Req #	Requirement Description	Threshold / Objective	Alternative
DAR-PR-1	EUDs must be provisioned over wired connections, or physically on the EUD.	T=O	
DAR-PR-2	When an EUD has been successfully provisioned, its identity (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) must be recorded in authorization databases.	T=O	
DAR-PR-3	The EUD must be loaded with an authorized software build during provisioning.	T=O	
DAR-PR-4	The EUD must be loaded with the Full Drive Encryption, File Encryptor, or Platform Encryptor during provisioning.	T=O	
DAR-PR-5	Services not authorized by the AO must be disabled during provisioning of the EUD.	T=O	

7.2 MOBILE ACCESS EUD PROVISIONING

Initial provisioning of the EUD can be performed using enrollment capabilities hosted in the Red Network, Gray Management Network, or a standalone management system with the same handling controls as the Gray Network. Certain circumstances require an EUD to connect to an online system for initial provisioning to enable the EUD to be fully provisioned. This initial provisioning may only be performed once, must occur before any other provisioning has been conducted, and only if required to provision the EUD. It must also perform only the minimally required provisioning steps needed to enable a traditional provisioning system (on the Red, Gray Management or standalone provision system) to complete the EUD's provisioning. To support different device types, it may be necessary to support both wireless and wired connection capabilities to the EUD being provisioned. If wireless provisioning is used, the WLAN Access System must be contained within a shielded enclosure, with 80 dB of attenuation across the frequency range from 2 to 6 GHz. The provisioning process includes assigning Government identifiers to the device, installing required applications, configuring the device's policy and settings, and loading certificates and keying material. Prior to provisioning devices, configuration profiles are created and required device applications are obtained.

Initial provisioning (for all device types) should include the following, in no specific order:

- **Device registration**. Collect identifying information from the EUD, assign Government device identifiers for the Gray and Red domains, and update data stores (directory, inventory, and/or authorization) to include the new EUD.
- **Settings configuration**. Load configuration (within the limitations of what is supported by each device type) that implements policies on allowed and disallowed services (such as Bluetooth) and user authentication parameters (i.e. password length and when to lock the device). Supply other settings such as network parameters.
- **Application installation**. Load required applications, including the VPN client and enterprise client applications. There is currently no support for an online application store, therefore, all applications should be loaded during initial provisioning. If possible, unneeded applications should be removed from the device.
- **Certificate request and issuance**. Using the assigned Government device identifiers, connect to the Gray Network, request certificates from the Outer CA, and load received material into the EUD. Disconnect the device from the Gray Network, connect to the Red Network, request certificates from the Inner CA, and load received material into the EUD.

  Note: It is possible for both CAs to reside on the Red Network or the certificate requests can be conducted through in an offline manner using a standalone provisioning network.

Depending on the EUD's capabilities, the device will either connect and interact with the signing CAs to be issued certificates, or the certificates will be generated and loaded onto a device storage medium from a provisioning workstation for transfer to the EUD. There will also be differences based on whether the EUD generates and provides a private key for the certificate, or is issued one from the CA (Note: more secure handling and transfer is required for the latter case).

DRAFT

777 Once the EUD is properly configured and certificates and keying material are in place, it is ready to be
778 issued to the user after the user login has been established and the user has been associated with the
779 device in the registration data. Once the device is connected to the Red Network, the device will be
780 classified.

781 **Table 12. MA CP EUD Provisioning Requirements (PR)**

Req #	Requirement Description	Threshold / Objective	Alternative
MA-PR-1	A Provisioning WLAN using WPA3-PSK authentication and encryption must be established on the Red Management Network, Gray Management Network, or standalone management network to support provisioning of EUDs.	T	MA-PR-4
MA-PR-2	If wireless provisioning is used, the Provisioning WLAN must be contained within a shielded enclosure that provides at least 80 dB of attenuation across the frequency range from 2 to 6 GHz.	T	MA-PR-4
MA-PR-3	EUDs must be provisioned over the provisioning WLANs.	T	MA-PR-4
MA-PR-4	EUDs must be provisioned over wired connections.	O	MA-PR-1 and MA-PR-2 and MA-PR-3
MA-PR-5	When an EUD has been successfully provisioned, its Government identifiers (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) must be recorded in authorization databases.	T=O	
MA-PR-6	The EUD must be loaded with an authorized software build during provisioning.	T=O	
MA-PR-7	The EUD must be loaded with VPN and TLS configuration profiles during provisioning.	T=O	
MA-PR-8	Services not authorized by the AO must be disabled during the provisioning of the EUD.	T=O	
MA-PR-9	If the EUD requires an initial vendor online provisioning process, this solution must be approved by the NSA.	T=O	
MA-PR-10	If the EUD requires initial vendor online provisioning, this onetime provisioning must only conduct minimal provisioning to enable a provisioning system within the CSfC boundary (Red, Gray or a standalone provisioning system) to complete the provisioning process.	T=O	

782

DRAFT

783 **Table 13. CWLAN CP EUD Provisioning Requirements (PR)**
784

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PR-2	The Provisioning WLAN on the Gray Management Network must be contained within a shielded enclosure that provides 80 dB of attenuation across the frequency range from 2 to 6 GHz.	T	WLAN-PR-5
WLAN-PR-3	The Provisioning WLAN on the Red Network must be contained within a shielded enclosure that provides 80 dB of attenuation across the frequency range from 2 to 6 GHz.	T	WLAN-PR-5
WLAN-PR-6	When an EUD has been successfully provisioned, its Government identity (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) must be recorded in authorization databases accessible to the WLAN Authentication Server.	T=O	

785

786 # 8 MULTIPLE SECURITY LEVELS

787 This section extends the MS levels use case found in MA to the CWLAN CP and adds additional
788 alternatives to the Extensive Authentication Protocol-Transport Layer Security (EAP-TLS) method within
789 the MA CP.

790 The purpose of the MS levels use case is to cover the necessary security requirements when deploying
791 multiple inner encryption components of different classifications within MA and CWLAN. The objective
792 of these requirements is to restrict the EUDs from connecting to the separate Inner Encryption
793 Components. This is a logical separation enforced by both the Outer Encryption Component and the
794 Gray Firewall. There are three distinct methods for achieving this separation. Each method focuses on
795 establishing the EUD's identity and having the Outer Encryption Component enforce separation. The
796 three methods for establishing EUD identity for this separation are:

797 - EAP-TLS: The EUD establishes an EAP-TLS session, brokered through the Outer Encryption
798 Component, to an Authentication Server within the Gray Management Network. This allows the
799 authentication server to set access parameters with the Outer Encryption Component.
800 - VPN pool or WLAN pool: Where a separate VPN Pool or WLAN pool exists for each distinct EUD
801 classification.
802 - Certificate Field: Places an additional field within the certificate to allow the Outer Encryption
803 Component to sort between the EUD's classification for separation.

804 Once the EUD's identity has been established by one of the three methods, the Outer Encryption
805 Component must assign the EUD to the respective internal network interface for its classification. Virtual
806 interfaces are permitted when they are cryptographically separated on the physical interface, such as
807 through a site-to-site IPsec tunnel between the Outer Encryption Component and the Gray Firewall,

DRAFT

provided the Outer Encryption component and Gray firewall are capable of a site-to-site tunnel as shown in Figure 21.

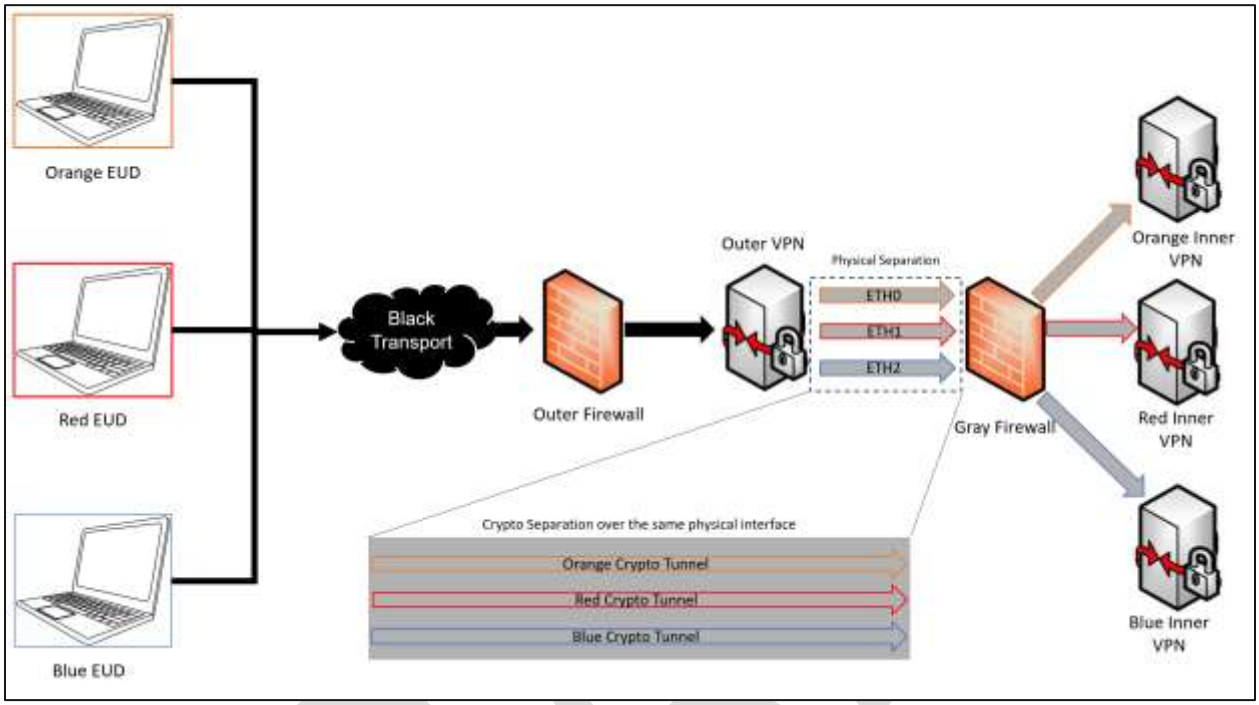


Figure 21. Multi-Inner Physical and Crypto Separation

Both the Outer Encryption Component and Gray Firewall must use either Access Control Lists (ACLs) or Virtual Routing and Forwarding (VRFs) for separation to ensure the EUDs cannot communicate with EUDs of a different classification. The Gray Firewall may allow for the EUDs to communicate with the Gray Data Plane services (i.e., DNS, Certificate Revocation List, Online Certificate Status Protocol (OCSP). The Gray firewall must then filter and route all the EUDs over its own dedicated interface to its respective Inner Encryption Component and ensure that the Inner Encryption Components cannot communicate with one another.

When implementing the MS level use case, all MS capabilities must be implemented, along with one of the MS-EAP, MS-POOL, or MS-CERT requirements.

Table 14. MA CP MS Level Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MS-1	The Outer VPN Gateway must assign a Firewall ACL or VRF to EUDs based on the attribute information provided by the authentication server, VPN Pool assignment, or Certificate Field.	MS	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MS-2	The Outer VPN Gateway must use unique physical internal interfaces for each enclave solution. VLAN trunking of multiple enclaves **is not** permitted.	MS	T=O	MA-PS-3
MA-MS-3	The Outer VPN Gateway must use a unique IPsec VPN tunnel between itself and the Gray Firewall for each enclave solution. VLAN trunking of multiple enclaves **is not** permitted.	MS	T=O	MA-PS-2
MA-MS-4	The Outer VPN Gateway must route EUD traffic over the appropriate interface, VPN tunnel, and network based on the attribute provided by the authentication server, VPN Pool, or certificate identifier.	MS	T=O	
MA-MS-5	The Outer VPN Gateway and Gray Firewall must assign a Firewall ACL to EUDs based on the attribute information provided by the authentication server, VPN Pool, or certificate identifier.	MS	T=O	
MA-MS-6	Gray Network components must be physically protected to the level of the highest connected classified network.	MS	T=O	
MA-MS-7	The solution must include an authentication server in the Gray Management Network.	MS-EAP	T=O	
MA-MS-8	A unique device certificate must be loaded on the authentication server along with the corresponding CA (signing) certificate.	MS-EAP	T=O	
MA-MS-9	The EUD must establish an EAP-TLS session with the Outer VPN Gateway within IKE to exchange credentials.	MS-EAP	T=O	
MA-MS-10	The Outer VPN Gateway must act as an EAP pass-through and forward the authentication packet between the EUD and authentication server.	MS-EAP	T=O	
MA-MS-11	Upon successful authentication, the authentication server must send an Access-Accept packet (Radius or Diameter) to the Outer VPN Gateway, including an attribute indicating the EUD's associated network.	MS-EAP	T=O	
MA-MS-12	The EUD and authentication server must use X.509 device certificates for mutual authentication.	MS-EAP	T=O	
MA-MS-13	The EUD and Outer VPN Gateway must use approved algorithms from Table 14 and process for Key Exchange.	MS-EAP	T=O	MA-MS-15
MA-MS-14	The EUD and Outer VPN Gateway must only use TLS Cipher Suites selected from Table 16 for encryption.	MS-EAP	T=O	MA-MS-16

DRAFT

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MS-15	The EUD and Outer VPN Gateway must use approved algorithms from Table 15 and process for key establishment.	MS-EAP	O	MA-MS-13
MA-MS-16	The EUD and Outer VPN Gateway must only use TLS Cipher Suites selected from Table 17 for encryption.	MS-EAP	O	MA-MS-14
MA-MS-17	The Outer VPN must maintain separate VPN Pools for each classification of EUDs.	MS-POOL	T=O	
MA-MS-18	The EUD's Certificate must contain a unique identifier that the Outer VPN uses to distinguish between EUDs of different classifications.	MS-CERT	T=O	

822

DRAFT

APPENDIX A. GLOSSARY OF TERMS

Black Network – A network that contains classified data that has been encrypted twice.

Capability Package (CP) – 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.

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

Dedicated Inner – A dedicated component that provides the inner layer of encryption and connects to the Red Compute Environment.

Dedicated Outer (DO) - A dedicated piece of hardware that can be part of an EUD and terminates the Outer layer of encryption.

End User Device (EUD) – A form-factor agnostic component of the MA 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.

Gray Network – A network that contains classified data that has been encrypted once (see Section 4.2.2).

Hardware-Separated – A configuration in which components are physically separate and operate on dedicated hardware.

Hypervisor – Software or firmware that creates and manages VMs by allocating and controlling access to underlying physical hardware. It allows multiple VMs to operate independently on a single physical system.

Keying Material – Information used to establish, maintain, or protect cryptographic operations.

Protection Profile (PP) – 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.

Provisioning – The process of configuring an EUD with required settings, user account information, certificates, keying material, and security configurations needed for the device to be issued to and used by an authorized user.

Red Network - Contains only Red data and is 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.

DRAFT

Retransmission Device (RD) – A standalone piece of hardware used to provide Black Network connectivity to EUDs.

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

Virtual EUD – An EUD that contains at least four VMs (End User Domain, Inner Encryption domain, Outer Encryption Domain and a Black Transport Domain) as described in Section 6.12.

Virtualization – The use of software to create separate virtual computing environments on a single physical device.

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.

DRAFT

APPENDIX B. ACRONYMS

Acronym	Meaning
ACL	Access Control List
AO	Authorizing Official
CA	Certificate Authority
CDS	Cross Domain Solutions
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Capability Package
CSfC	Commercial Solutions for Classified
CWLAN	Campus Wireless Area Network
DAR	Data-At-Rest
DiT	Data-in-Transit
DNS	Domain Name Server
DoW	Department of War
DTLS	Datagram Transport Layer Security
EAP-TLS	Extensive Authentication Protocol-Transport Layer Security
ESP	Encapsulating Security Payload
EUD	End User Device
GPCP	General Purpose Compute Platform
GPOS	General Purpose Operating System
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
KVM	Keyboard, Video, Mouse
MA	Mobile Access
MA CP	Mobile Access Capability Package
MACsec	Media Access Control Security
MDF	Mobile Device Fundamentals
MS	Multiple Security
NIAP	National Information Assurance Partnership
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
PSK	Pre-Shared Key
RD	Retransmission Device
SA	Security Administrator
SSH	Secure Shell
SWaP	Size, Weight, and Power
TLS	Transport Layer Security
USB	Universal Serial Bus
VM	Virtual Machine

DRAFT

Acronym	Meaning
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA3	Wi-Fi Protected Access 3

866

DRAFT

867 # APPENDIX C. REFERENCES

Document	Title	Date
CNSSP 7	*CNSS Policy (CNSSP) Number 7, National Policy on the Use of Commercial Solutions to Protect National Security Systems*	December 2015
CNSSP 11	*CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Cybersecurity and Cybersecurity-Enabled Information Technology Products and Services*	February 2025
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Policy on the Use of Public Standards for Secure Information Sharing (CNSA 2.0)*	March 2025
DoDI 8420.01	*Commercial Wireless Local-Area Network Devices, Systems, and Technologies.* Office of the CIO of the DOD	November 2017
IPsec VPN Client PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*.	Latest Version
MA CP	CSfC Mobile Access Capability Package 2.8.0	March 2026
CWLAN CP	CSfC Campus WLAN Capability Package 3.2.0	March 2026
ConMon Annex	CSfC Continuous Monitoring Annex v1.1.0	March 2023
DAR CP	CSfC Data-at-Rest Capability Package v5.1.0	March 2026

868

869

870

871

DRAFT