


NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

EUD Composition Guidance Addendum 1.0

Draft 1

Version 1.0 Draft 1
5 May 2023


CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) EUD Composition Guidance Addendum	1.0 Draft 1	5 May 2023	• Initial Draft of the EUD Composition Guidance

Table of Contents

Table of Figures

List of Tables

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 WLAN (CWLAN), and Data at Rest (DAR) CPs* that conveys a structural change to End User Devices (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.

If a component is modified, NSA's CSfC Program Management Office (PMO) requires a statement from NIAP that states the modification does not alter the certification, or the security of the component. Modifications that trigger the revalidation process include, but not limited to configuring the component in a manner different from its NIAP-validated configuration and modifying the Original Equipment Manufacturer's code (to include digitally signing the code).

2 PURPOSE AND USE

This Addendum 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 (https://www.nsa.gov/resources/commercial-solutions-for-classified-program), to compose an EUD to meet the requirements 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 this CP, all Threshold (T) Requirements, or the corresponding Objective (O) Requirements applicable to the selected capabilities, must be implemented.

Please provide comments on usability, applicability, and/or shortcomings to your NSA Client Advocate and the Addendum Maintenance Team at CSfC_Addendum@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, DoD customers must follow DoDI 8540.01 when deploying a CDS within a CSfC solution and if any discrepancies are found between the guidance in this document and DoDI 8540.01 report according to the instruction found in this section.

3 LEGAL DISCLAIMER

This Addendum 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 must 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 Addendum, even if advised of the possibility of such damage.

The user of this Addendum 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 Addendum is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 OVERVIEW

This Addendum describes a structural change to EUDs that clarifies the usage of technologies, product selections, and other changes within the MA, CWLAN, and DAR CPs. The following changes will be made to the overall CSfC program. Additional components will be added to the CSfC Components List to allow for this new change. Detail the usage of these new components on the CSfC Components List within MA, CWLAN, and DAR CPs. Using virtualization and other such software separation technologies within CSfC. Expand the usage of hardware separation within EUD. Clarify the deployment, usage, and approvals of Access CDS as EUDS within the CSfC Program.

Table 1 is a summary of the EUD types which are explained and presented within this document. For further information on these EUD types can be found in sections 6, 7, 8, and 10.

74 **Table 1. EUD Summary**

Sub-Component	Description	Note
Base Composed EUDs and MDF EUDs	An EUD built to function within the constraints of a typical OS or MDF system	Minimum standard for EUD in CSfC
Software Separated EUD: EUD with Containerization	An EUD built around a standard OS with a containerization engine running to abstract out critical functions into separate namespaces	Offers more usability but no difference in security than base EUD
Software Separated EUD: EUD with Virtualization	An EUD built around a Hypervisor without hardware abstraction used to separate critical functions critical components into separate virtual instances	Offers more usability and a marginal increase to security.
Software Separated EUD: Separation Kernel	An EUD built around a separation kernel and relies on the kernel to segment out critical functions	Offers extremely low level isolation
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 function are physically separated out into separate hardware of the EUD

75

76 ## 4.1 COMPOSED EUD PRODUCT SELECTIONS

77 Currently in the CSfC Program there are two options on how to be listed on the CSfC Components list: 1)
78 meet all requirements within National Information Assurance Partnership's (NIAP) Protection Profile
79 (PP) for Mobile Device Fundamentals (MDF) with the CSfC selectors; 2) meet all requirements from the
80 following PP and PP Extended Package:

81 - General Purpose Operating Systems (GPOS) PP with all CSfC Selectors
82 - MDF PP EP Wireless Local Area Network (WLAN) Clients
83 - MDF PP EP Software/Hardware Full Drive Encryption
84 - (Optional) PP Module for Virtual Private Network (VPN) Client

85 The EUD going through either of these methods to become a listed EUD component requires a single
86 vendor to either own each component within a EUD or become responsible for the security and
87 updating of such components. This has led to only MDF PP devices to be listed on the CSfC Components

List this causes all other devices cannot be used within a CSfC Solution without additional deviation approvals.

This addendum replaces the second method with a composed EUD model. Instead of listing individual devices that can act as EUDs on the CSfC Components List, the sub-components which make up these EUDs will be listed on the CSfC Components List. The responsibility of selecting and composing these sub-components into a functioning EUDs is up to the customer and/or Trusted Integrator. The CSfC Program does not guarantee the interoperability of the different sub-components. The sub-components that make up a composed EUD include the following:

- GPOS PP with all CSfC Selectors
    - PP Module WLAN Clients (CWLAN Only)
- Virtualization PP (Virtual EUDs Only)
    - PP Module for Client Virtualization
- General Purpose Compute Platform (GCPP) PP
- Dedicated Security Component PP (Optional)
- Full Drive Encryption – Authorization Acquisition PP and Full Drive Encryption - Encryption Engine PP (Optional)

For more details on these individual sub-components see Section 5.

4.2 Composed EUD Types of EUDs.

The Composed EUD is made up of multiple NIAP tested components as listed in Section in 4.1. The core protection profiles that make up a composed EUD are the GPCP PP and GPOS PP which are used to establish trust within the operation and interactions between the OS and hardware platform. There are three types of Composed EUDs which are used within the MA CP and CWLAN they are:

- IPsec-IPsec EUD, referred to as VPN EUD in MA CP
- IPsec-TLS EUD, referred to as TLS EUD in MA CP
- WLAN-IPsec EUD, referred to as a WLAN EUD in CWLAN CP

Section 6 details the overall concept of the Composed EUD and the individual types of Composed EUD.

4.3 Virtual Composed EUDs

Virtualization is a technology that has widely been adopted within the CSfC Program to improve the security and capability of the EUDs. Virtualization can be leveraged on either Composed EUDs or on MDF EUDs. The target for virtualization within CSfC is a Type One Hypervisor where the virtualization engine runs directly on the hardware platform instead of running on a separate OS. This particular Type One Hypervisors that are being targeted have a great deal of separation which includes kernel separation

and limited hardware separation. To meet this target for this separation a Type One Hypervisor must meet the Protection Profile for Virtualization and the PP-Modules for Client Virtualization.

For more information on the Virtual Composed EUDs see section 7.

4.4 Software Separated EUDs

Software Separated EUDs is a category of technologies that offers some form of separation to a Composed EUD but does not meet the strict Type 1 Hypervisor requirements for a Composed Virtualized EUD. These technologies can include containerization, and virtualization which does not meet with CSfC requirements for Virtualized EUDs in Section 7, and other software separation technologies. These currently do not have particular protection profiles written for them and therefore cannot be tested for their exact functionality. All software separation technologies must be tested against the GPOS PP and the security features of these technologies above those within the GPOS will not be considered on an architectural level for CSfC solution but may be considered for individual solution deployments.

For more information on the Virtual Composed EUDs see section 8.

4.5 DAR EUDs

The DAR CP is used to provide an additional layer of security to CSfC data in transit EUDs ensuring that their data is secure at rest. Virtualization, containerization and security separation kernel technologies are becoming more prevalent with CSfC Data-in Transit (DiT) solutions. DAR must have provisions and guidance on how its guidance applies to these solutions. The following table summarizes the general use cases within the DAR CP all of which are applicable to a Composed EUD:

Table 2. DAR Solution Design Summary

Solution Design	Designator	Description
SWFDE/FE	SF	DAR solution design that uses FE (File Encryption) as the inner layer and SWFDE (Software Full Disk Encryption) as the outer layer
PE/FE	PF	DAR solution design that uses FE as the inner layer and PE (Platform Encryption) as the outer layer
HWFDE/FE	HF	DAR solution design that uses FE as the inner layer and HWFDE as the outer layer
HWFDE/SWFDE	HS	DAR solution design that uses SWFDE as the inner layer and HWFDE (Hardware Full Disk Encryption) as the outer layer
HWFDE/HWFDE	HH	DAR solution design that uses HWFDE as the inner layer and HWFDE as the outer layer

SWFDE/SWFDE	S2	DAR solution design that uses SWFDE as the outer layer and SWFDE as the inner layer

Within a Composed EUD concept the validation of the OS, Hypervisor, and physical hardware of the EUD are core to the security of these devices. Within the DAR CP it is highly recommended that the OS and Hypervisor are from the CSfC Components list but not the hardware platform. The reason is that the DAR components may rely upon the OS functions to perform various security services and ensure that the data is properly contained within the virtual machine.

For more information and details on DAR EUDs see Section 9.

4.6 Hardware Separated Composed EUDs

Within the CSfC architecture, especially the MA CP, there is the concept of multiple components making up a single EUD. This concept is exemplified by the retransmission device (RD) and the Dedicated Outer VPNs which can be paired with a traditional EUD. This is done to pass along both functionality and risk to a separate component other than the EUD or to have the separate component perform a function that the EUD is incapable of doing. This concept can be expanded on to further enhance the security of an EUD or allow for EUDs that cannot meet the requirements placed on traditional EUD such as a laptop, smartphone, tablet, or computer.

For more information and details on Hardware Separated Composed EUD see Section 10.

4.7 Access Cross Domain Solution Composed EUDs

As the use of EUD based Access Cross Domain Solutions (CDS) within CSfC Solutions becomes more common, uniform guidance on how they may be deployed as CSfC EUDs. Access CDSs are being used within CSfC solutions to fully replace a traditional EUD. Thus, the NCDSMO and the CSfC Program have partnered, to allow for reciprocity between the NCDSMO Baseline and the CSfC Components List. The specific CDS that is targeted here is the Access CDS that relies of virtualization technologies for separation of different domains which are similar to Virtualized EUDs discussed in Section 7. For any additional information on CDS contact the NCDSMO at ncdsmo@nsa.gov. For questions on what Access CDS can be used as a CSfC EUD contact csfc@nsa.gov.

For more information and details on the usage CDSs as EUDs within CSfC Solutions see Section 11.

5 PRODUCT SELECTIONS

The new scheme for composing EUDs requires the customer or Trusted Integrator to select validated sub-components composing the EUD. The exact sub-components required to compose an EUD in each CP and individual use case will be detailed in subsequent sections. This section focuses on the details of the sub-components themselves. The details will include the NIAP PP governing component, the functionality, and intended use of the component. The following sub-components will be added to the CSfC Components list:

- EUD Hardware Platform
- Dedicated Security Component

- Operating System
- Hypervisor

5.1 EUD Hardware Platform

The EUD Hardware Platform is the physical hardware that the other sub-components of the EUD operate. All Composed EUDs must have an EUD Hardware Platform that has gone through the *GPCP PP* and be listed on the CSfC Components list as a EUD Hardware Platform. The platform typically is a traditional laptop, computer, tablet, phone or other such end user form factor, but may also be a server or other computing form factor.

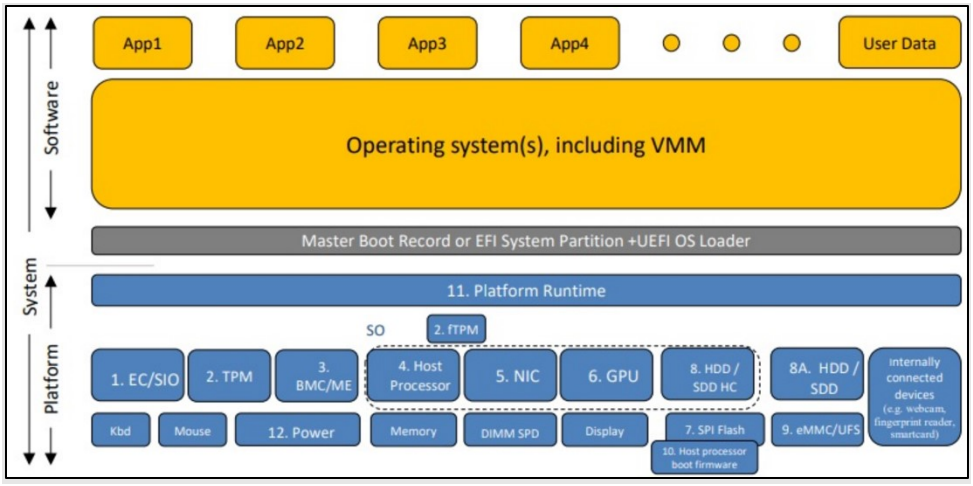


Figure 1. General Purpose Computing Platform

This platform is a collection of hardware devices and firmware that provides the functional capabilities and services needed by tenant software. Such components typically include embedded controllers, trusted platform modules, management controllers, host processors, network interface controllers, graphics processing units, flash memory, storage controllers, storage devices, boot firmware, runtime firmware, human interface devices, and a power supply. The EUD serves as the basis for all other EUD components to operate on and includes laptops, tablets servers, and other computing devices.

5.2 Dedicated Security Component

The Dedicated Security Component (DSC) is a combination of a hardware component and its controlling firmware that provides a secure execution environment, key storage and/or other security related functionality to the composed EUD. Currently, a DSC is not required but an objective sub-component that will further enhance the security of an EUD and is governed by the *Dedicated Security Component cPP.* These DSCs should take the form of Secure Elements (SE), Trusted Platform Modules (TPM), Hardware Security Modules (HSM), Trusted Execution Environments (TEE), and Secure Enclave Processors (SEP). The firmware of these should provide the encompassing platform with services for the provisioning, protection, and use of Security Data Objects (SDOs), which include keys, identities, attributes, and other types of Security Data Elements (SDEs).

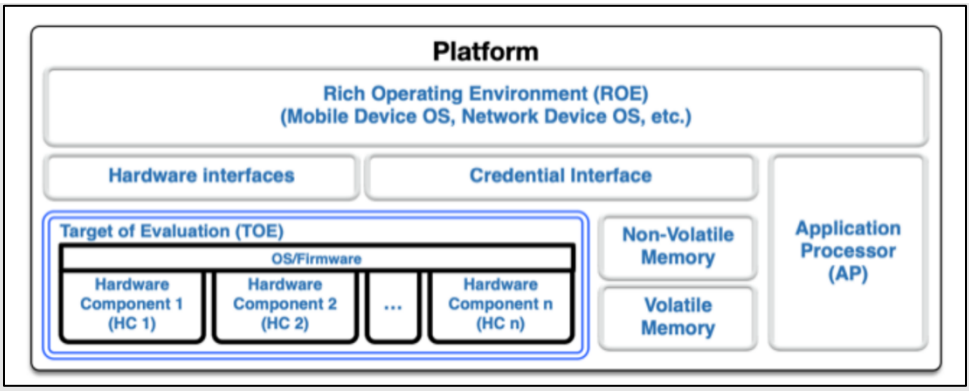


Figure 2. Dedicated Security Component

It is expected that the DSC will be integrated into the EUD Hardware Platform and thus the Hardware Platform will be tested against *Dedicated Security Component cPP* or have an already tested DSC integrated into it. Additionally, *MDF cPP* EUDs can leverage the DSCs to provide the same functionality as the composed EUDs. Long term, the CSfC Program will require that DSC's be validated against the *Dedicated Security Component cPP* and to be integrated into every EUD. As of now having a DSC is an objective design feature for all EUDs.

5.3 Operating System

The Operating System (OS) is software that manages computer hardware and software resources for EUDs and provides common services for application programs. The hardware it manages may be physical or virtual. The OS encompasses the OS kernel and its drivers, shared software libraries, and some application software included with the OS. Applications included are those that provide essential security services, many of which run with elevated privileges. The OS is governed by the *Protection Profile for General Purpose Operating Systems*.

5.4 Wireless Local Area Network Client

The WLAN Client describes how the security functionality of the 802.11 wireless networking interface and driver interacts with the OS. The WLAN Network Client is a sub-component of the OS and should be paired with the given OS. The WLAN Network Client is governed by the *PP-Module for Wireless Local Area Network Client*. The WLAN Client describes the security functionality of the 802.11 hardware and drivers controlled by an OS to connect to a WLAN Access System.

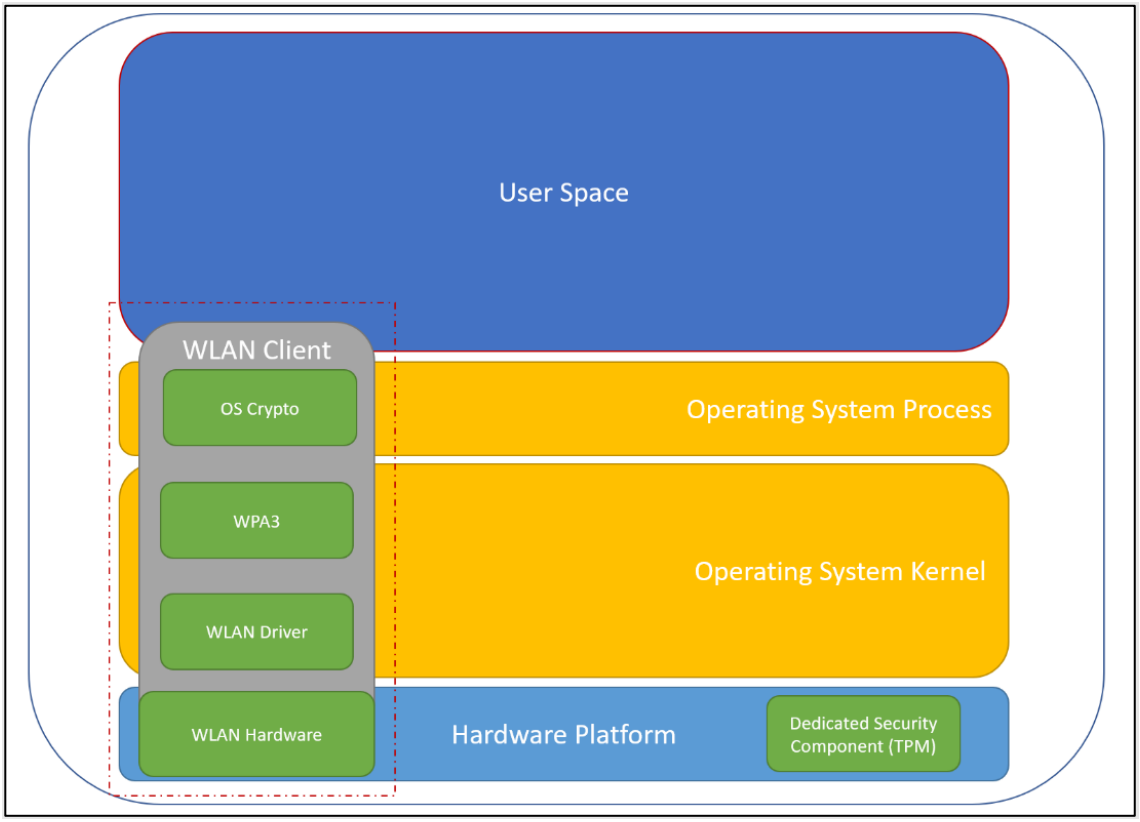


Figure 3. WLAN Client

5.5 HYPERVISOR

The Hypervisor, also referred to as the Client Virtualization, is a virtualization that runs on the EUD hardware in place of an OS and its Kernel. It runs additional guest operating systems and their guest kernels. The Hypervisor used is considered to be a Type One hypervisor where the virtualization engine directly runs on the hardware platform instead of running on a separate OS. The Type One Hypervisor has a great deal of high-level separation that includes kernel separation and limited hardware separation. The Hypervisor is governed by the *Protection Profile for Virtualization* and the *PP-Modules for Client Virtualization*.

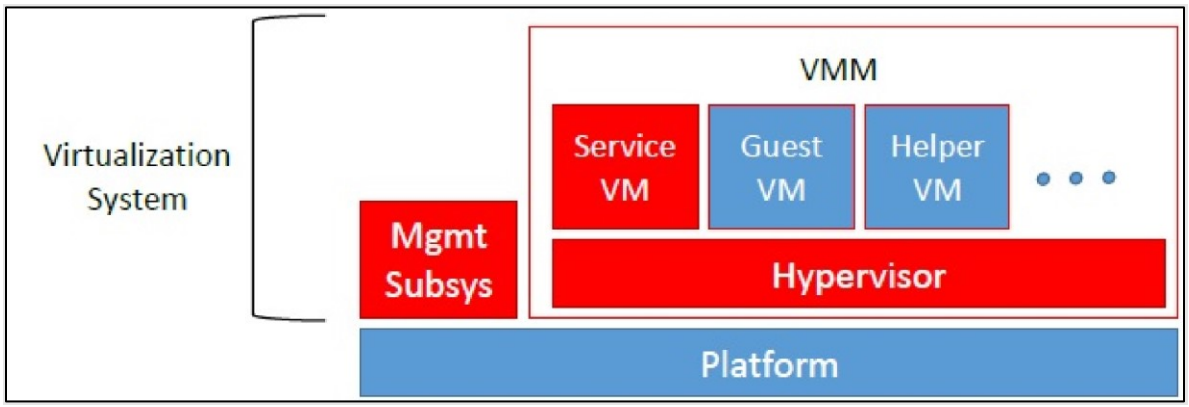


Figure 4. Virtualization Client

5.6 End User Device Encryption

EUD encryption encrypts a set of user-selected data. For ease of explanation, "file" will frequently be used to refer to the encrypted object (however, the encrypted object could be any number of things - folders, volumes, containers, etc.). EUD encryption is another sub-component of the OS and should be paired with the given OS. EUD encryption is governed by the *PP-Module for File Encryption.* While this PP specifies file encryption in general, it also applies to EUD encryption.

Device encryption captures most of the storage medium, including all user files. The Full Disk Encryption (FDE) collaborative Protection Profiles describe the requirements and assurance activities necessary for the actual encryption/decryption of the data by the DEK. Each PP will also have a set of core requirements for management functions, proper handling of cryptographic keys, updates performed in a trusted manner, audit, and self-tests. The device encryption is governed by the *Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine.* Both cPPs are required for a fully evaluated FDE product, they may be two separate products working together or one product with both evaluations.

5.7 Virtual Private Network Client

The Virtual Private Network (VPN) Client, a software application that runs on the OS, establishes a secure IPsec connection between the host platform and a remote system. The VPN client is located outside or inside of a private network and establishes a secure tunnel to an IPsec peer. IPsec peers are defined as:

- VPN gateways
- Other VPN clients
- An IPsec-capable network device (supporting IPsec for the purposes of management)

The tunnel provides confidentiality, integrity, and data authentication for information that travels across a less trusted (sometimes public) network. All VPN clients that comply with this document will support IPsec. The VPN Client is governed by the *PP-Module for VPN Client*.

5.8 Transport Layer Security Application

The Transport Layer Security (TLS) Application is a general application that has TLS evaluated, such as a Voice and Video over IP (VVoIP) application or an email application that runs on the OS. The TLS Application located outside or inside of a solution and establishes a secure connection to an TLS peer. TLS peers are defined as:

- TLS Server
- VoIP Server
- Email Server

The secure connection provides confidentiality, integrity, and data authentication for information that travels across a less trusted (sometimes public) network. The TLS Application is governed by the Protection Profile for Application Software Version and the Functional Package for TLS.

6 COMPOSED EUD

The Composed EUD is an alternative to the *MDF PP* where the EUD is composed of multiple NIAP tested components. The two core PPs that the composed EUDs rely on are the *GPCP PP and GPOS PP* which are used to establish trust within the operation and interactions between the OS and the hardware platform. This section details a composed EUD based on these two components while Composed EUDs which rely on virtualization technology will be detailed in Section 7.

There are three types of Composed EUDs used in the MA and CWLAN CPs:

- IPsec-IPsec EUD, referred to as VPN EUD in MA CP
- IPsec-TLS EUD, referred to as TLS EUD in MA CP
- WLAN-IPsec EUD, referred to as a WLAN EUD in CWLAN CP

6.1 IPSEC-IPSEC EUDS

IPsec-IPsec EUDs use two IPsec tunnels to connect to the Red Network. Such an EUD includes both an Inner VPN Client and Outer VPN Component to provide the two layers of IPsec. Throughout this addendum, the IPsec-IPsec EUD design is referred to as the "VPN EUD." VPN EUDs can be implemented using combinations of IPsec VPN Clients and IPsec Gateways. For example, a VPN EUD can be implemented on a Computing Device with two VPN Clients on the same stacks. The Black Transport for this EUD can be any government owned wireless transport that the AO approves or retransmission device as detailed in the relevant CP.

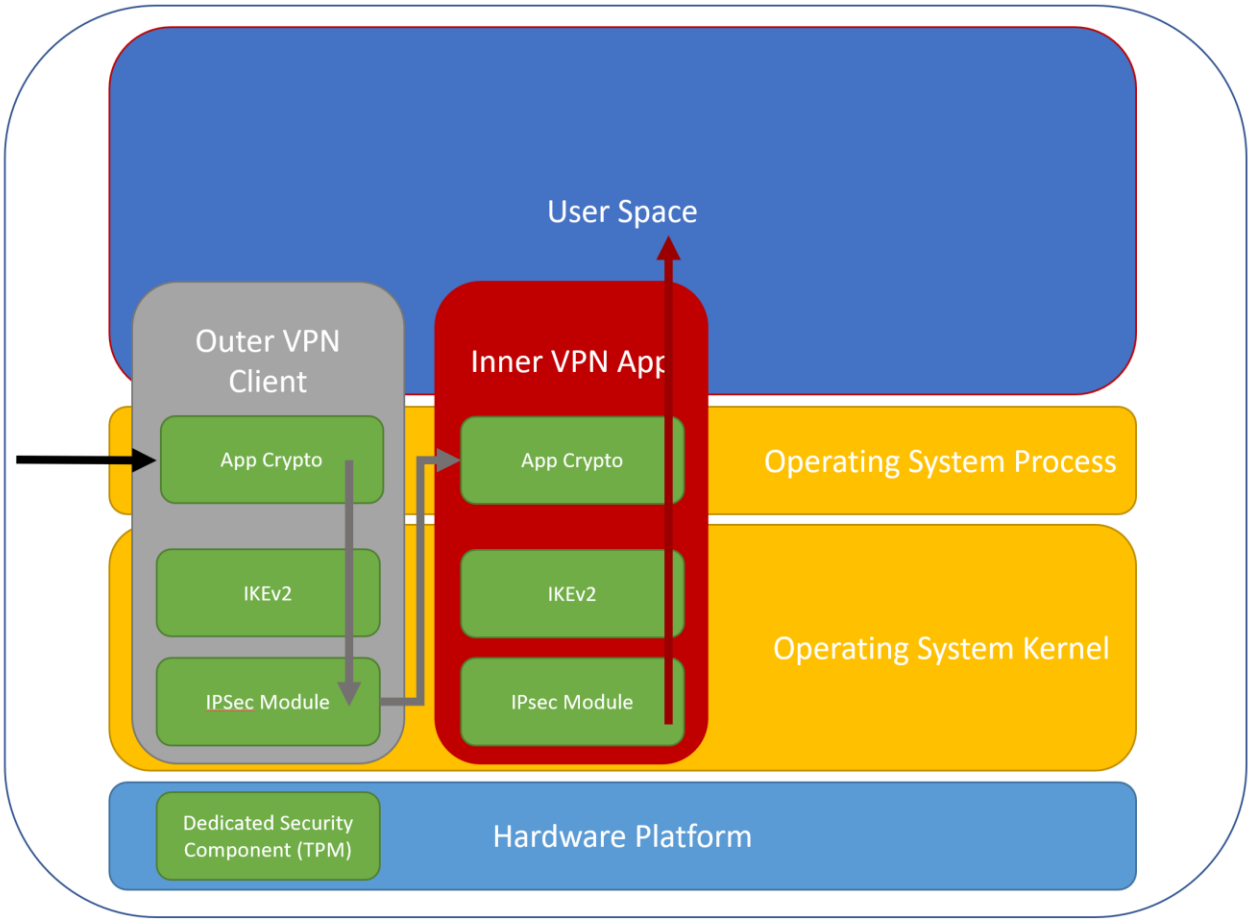


Figure 5. IPsec-IPsec EUD

A logical diagram of the components of the VPN EUD can be seen in Figure 5. The EUD itself is run on physical hardware from the PP for GPCP. The hardware may have a dedicated security component integrated with it that is chosen from the Collaborative Protection Profile for Dedicated Security Component. The EUD's OS must be chosen from the Protection Profile for GPOS. The two VPN Clients must be chosen from the PP-Module for VPN Client and tested on the EUD's OS. The EUD's encryption must be an encryptor chosen from the Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine.

Table 3. IPsec-IPsec EUD Components

Component	Protection Profile
EUD Hardware	*Protection Profile for General Purpose Computing Platform*
EUD-Dedicated Security Component (Optional)	*Collaborative Protection Profile for Dedicated Security Component*
OS	*Protection Profile for General Purpose Operating Systems*

Outer VPN Client	*PP-Module for VPN Client*
Inner VPN Client	*PP-Module for VPN Client*
EUD Encryption	*Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*

6.2 IPSEC-TLS EUDS

IPsec-TLS EUDs use an Outer layer of IPsec encryption and an Inner layer of TLS encryption to access the Red Network. Throughout this document, the IPsec-TLS EUD design is referred to as the "TLS EUD." The EUD's TLS Client includes various options that can be selected in accordance with the CP requirements to meet the operational needs of the customer. The EUD's TLS Clients include, but are not limited to, web browsers, email clients, and VVoIP applications. Traffic between the TLS EUD Client and the TLS-Protected Server is encrypted with TLS. The Black Transport for this EUD can be any government owned wireless transport that the AO approves or retransmission device as detailed in the relevant CP.

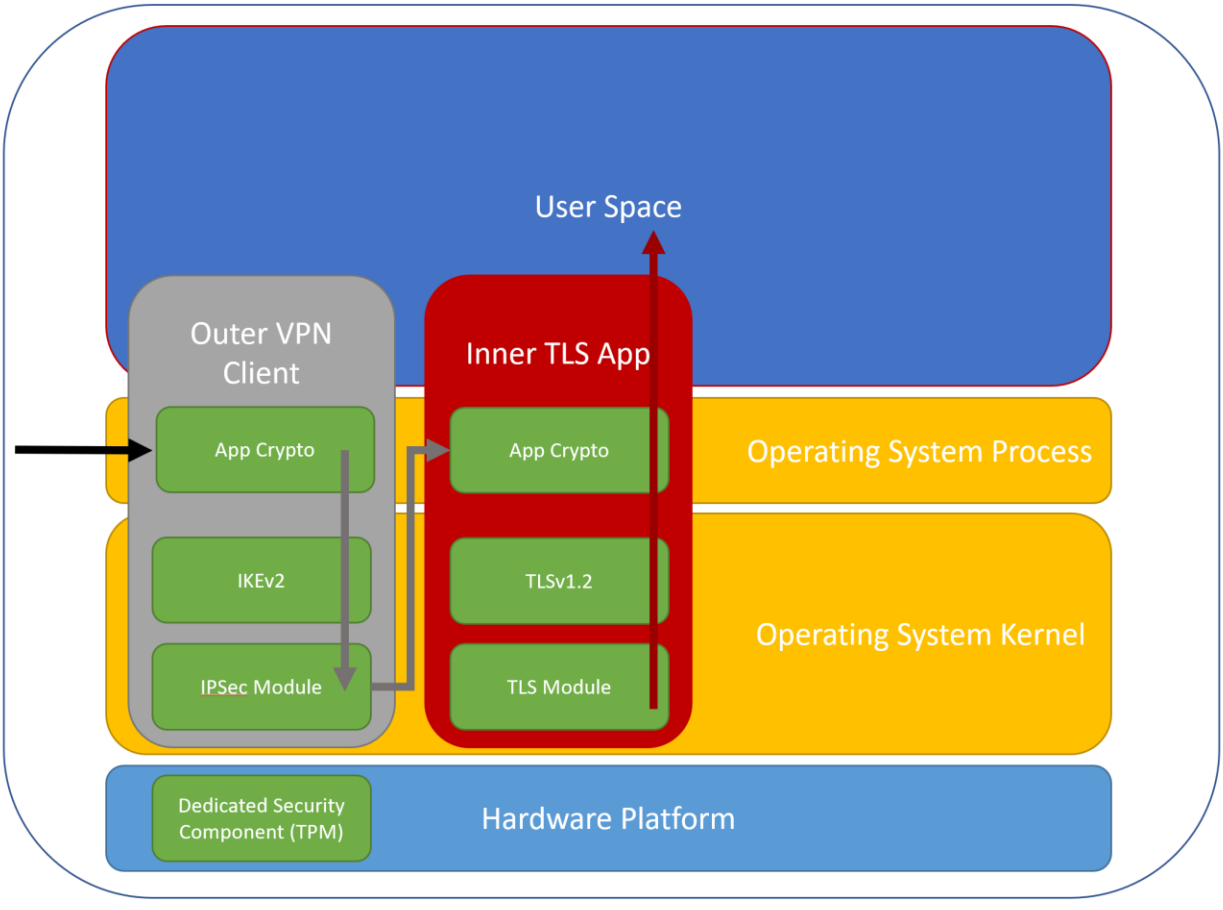


Figure 6. IPsec-TLS EUD

A logical diagram of the components of the TLS EUD can be seen in Figure 6. The EUD itself runs on physical hardware from the PP for GPCP. The hardware may integrate a dedicated security component that is chosen from the Collaborative PP for DSC. The EUD's OS must be chosen from the PP for GPOS. The VPN Client and TLS App must be chosen from any of the following PPs: Functional Package for TLS, PP-Module for VVoIP, or Extended Package for Email Clients. It must also be tested on the EUD's OS. The VPN Client must be chosen from the PP-Module for VPN Client and additionally be tested on the EUD's OS. For encryption, the EUD must use an encryptor that is chosen from the Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine.

Table 4. IPsec-TLS EUD Components

Component	Protection Profile
EUD Hardware	*Protection Profile for General Purpose Computing Platform*
EUD-Dedicated Security Component (Optional)	*Collaborative Protection Profile for Dedicated Security Component*
OS	*Protection Profile for General Purpose Operating Systems*
Outer VPN Client	PP-Module for VPN Client
Inner TLS Application	*Protection Profile for Application Software and, Functional Package for TLS* or *PP-Module for Voice and Video over IP (VVoIP)* or *Extended Package for Email Clients.*
EUD Encryption	*Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine.*

6.3 WLAN-IPsec EUDs

WLAN-IPsec EUD, or WLAN- VPN EUD, uses Wi-Fi Protected Access 3 (WPA3) and an IPsec tunnel to connect to the Red Network. Such an EUD includes both an Inner VPN Client and a WLAN client to provide the two layers of encryption. The WPA3 must minimally operate in WPA3-Personal mode or preferably in WPA3-Enterprise 192-bit mode. WLAN VPN EUDs can be implemented using combinations of IPsec VPN Clients and WLAN Access Systems. For example, a VPN EUD can be implemented on a Computing Device with the WPA and IPsec Encryption running on separate IP stacks. The WLAN VPN EUD is expected to be used with a Campus WLAN solution.

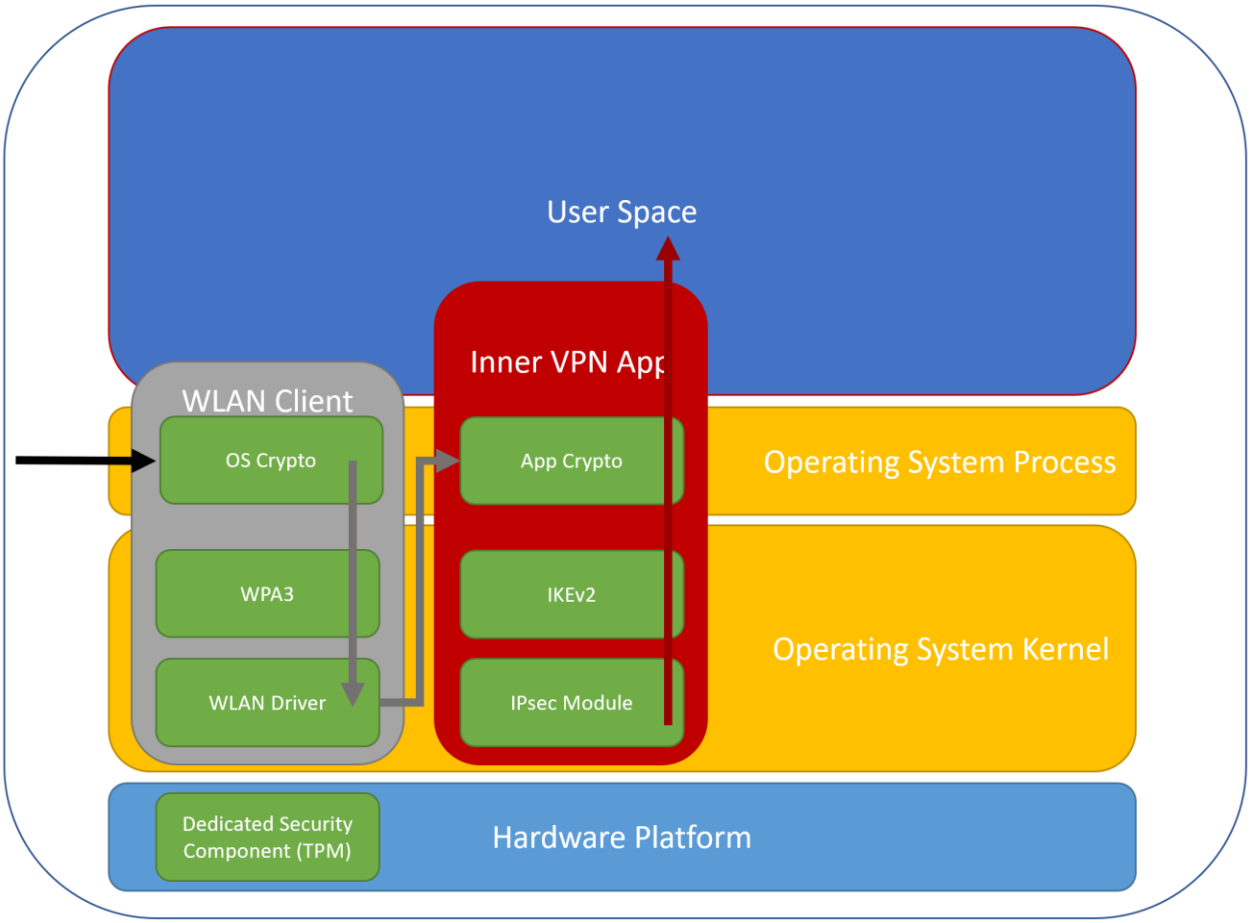


Figure 7. WLAN-IPsec VPN EUD

A logical diagram of the components of the WLAN VPN EUD can be seen in Figure 3. The EUD itself is run on physical hardware from the PP for GPCP. The hardware may integrate a dedicated security component that is chosen from the Collaborative PP for DSC. The EUD's OS must be chosen from the Protection Profile for GPOS. The WLAN Client must be chosen from PP-Module for WLAN Client and be tested on the EUD's OS. The VPN Client must be chosen from the PP-Module for VPN Client and be tested on the EUD's OS. For encryption, the EUD must use an encryptor chosen from the Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine.

Table 5. WLAN-IPsec EUD Components

Component	Protection Profile
EUD Hardware	*Protection Profile for General Purpose Computing Platform*
EUD-Dedicated Security Component (Optional)	*Collaborative Protection Profile for Dedicated Security Component*
OS	*Protection Profile for General Purpose Operating Systems*

WLAN Client	*PP-Module for Wireless Local Area Network (WLAN) Client*
Inner VPN Client	*PP-Module for VPN Client*
EUD Encryption	*Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*

340 ## 6.4 MOBILE ACCESS REQUIREMENTS

341 Mobile Access Product Selection Requirement the following table is a list of product selection
342 requirements which will be appended or changed to the MA CP as part of the EUD Composition Update.

343 **Table 6. Mobile Access Production Selection Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MA-PS-6	If using a MDF EUD, products used for Mobile Platform EUDs must be chosen from the list of Mobile Platforms on the CSfC Components List.	T=O	MA-PS-34 and (MA-PS-35 or MA-PS-33)
MA-PS-33	If using a composed EUD, the EUD's Hypervisor must be chosen from the list of Client Hypervisors on the CSfC Components List.	T=O	MA-PS-6 or MA-PS-35 or MA-PS-37
MA-PS-34	If using a composed EUD, the EUDs Hardware Platform must be chosen from the list of Hardware Platforms on the CSfC Components List.	T=O	MA-PS-6
MA-PS-35	If using a virtualized EUD, he EUD's Operating System used must be chosen from the list of Operating Systems on the CSfC Components List.	T=O	MA-PS-6 or MA-PS-33 or MA-PS-38
MA-PS-36	The EUD must have a Dedicated Security Component chosen from the list of Dedicated Security Components on the CSfC Components List.	O	Optional
MA-PS-37	If using an Access CDS EUD, The EUDs Hardware Platform must be validated as part of an Access CDS listed on the CDS Baseline.	T=O	MA-PS-33
MA-PS-38	If using an Access CDS EUD, The EUD's Hypervisor used must be validated as part of an Access CDS listed on the CDS Baseline.	T=O	MA-PS-35
MA-PS-39	The products used for the SWFDE layer must be chosen from the list of SWFDEs on the CSfC Components List.	T=O	MA-PS-40
MA-PS-40	The products used for the HWFDE layer must be chosen from the list of HWFDEs on the CSfC Components List.	T=O	MA-PS-39

344

6.4.1 MA EUD REQUIREMENT

The following table lists MA CP requirements that will be appended or changed as part of the EUD Composition Update.

Table 7. MA EUD Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
MA-EU-32	If an NSA-approved DAR Solution is not implemented on the EUDs, the MDF EUD must have the native platform DAR protection enabled.	T=O	MA-EU-82
MA-EU-82	If an NSA-approved DAR Solution is not implemented on the EUDs, the Composed EUD must have a layer of Software Full Disk Encryption or Hardware Full Disk Encryption Enabled.	T=O	MA-EU-32

6.5 CAMPUS WLAN REQUIREMENTS

The following table is a list of product selection requirements that will be appended or changed to the CWLAN CP as part of the EUD Composition Update.

Table 8. Campus WLAN Production Selection Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PS-3	The products used for any WLAN Client must be chosen from a Mobile Platforms or Operating Systems listed on the CSfC Components List for WLAN Clients.	T=O	WLAN-PS-21
WLAN-PS-4	If using a MDF EUD, the products used for Mobile Platform EUDs must be chosen from the list of Mobile Platforms on the CSfC Components List.	T=O	WLAN-PS-17 and (WLAN-PS-18 or WLAN-PS-19)
WLAN-PS-17	If using a composed EUD, the EUDs Hardware Platform must be chosen from the list of Hardware Platforms on the CSfC Components List.	T=O	WLAN-PS-4
WLAN-PS-18	If using a composed EUD, the EUD's Operating System used must be chosen from the list of Operating Systems on the CSfC Components List.	T=O	WLAN-PS-4 or WLAN-PS-19 or WLAN-PS-22
WLAN-PS-19	If using a virtualized EUD, the EUD's Hypervisor must be chosen from the list of Client Hypervisors on the CSfC Components List.	O	WLAN-PS-4 or WLAN-PS-18 or WLAN-PS-23
WLAN-PS-20	The EUD must have a Dedicated Security Component chosen from the list of Dedicated Security Components on the CSfC Components List.	O	Optional

WLAN-PS-22	If using an Access CDS EUD, The EUDs Hardware Platform must be validated as part of an Access CDS listed on the CDS Baseline.	T=O	WLAN-PS-18
WLAN-PS-23	If using an Access CDS EUD, The EUD's Hypervisor used must be validated as part of an Access CDS listed on the CDS Baseline.	T=O	WLAN-PS-19
WLAN-PS-24	The products used for the SWFDE layer must be chosen from the list of SWFDEs on the CSfC Components List.	T=O	WLAN-PS-25
WLAN-PS-25	The products used for the HWFDE layer must be chosen from the list of HWFDEs on the CSfC Components List.	T=O	WLAN-PS-24

6.5.1 WLAN EUD REQUIREMENT

The following table lists WLAN CP requirements that will be appended or changed as part of the EUD Composition Update.

Table 9. WLAN EUD Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-24	If an NSA-approved DAR Solution is not implemented on EUDs, the MDF EUD must have the native platform DAR protection enabled.	T=O	MA-EU-82
MA-EU-48	If an NSA-approved DAR Solution is not implemented on EUDs, the Composed EUD must have a layer of Software Full Disk Encryption or Hardware Full Disk Encryption Enabled.	T=O	MA-EU-32

7 VIRTUALIZED EUDS

Virtualization technology is being widely adopted within the CSfC Program to improve the security and capability of the EUDs. Virtualization can be leveraged on either Composed EUDs or on MDF EUDs. This virtualization relies on a Type One Hypervisor where the virtualization engine runs directly on the hardware platform instead of running on a separate OS. The Type One Hypervisor has a great deal of high-level separation that includes kernel separation and limited hardware separation. To meet the high bar for this separation a Hypervisor must meet the PP for Virtualization and the PP-Modules for Client Virtualization. If a Hypervisor cannot meet the PPs requirements, then it is considered a Software Separated EUD which is detailed in Section 8.

Virtualized EUD can be used to enhance the Composed EUDs discussed in Section 6 and can additionally be used to enhance MDF based EUDs. Type One Hypervisors provide additional security for the component by isolating the storage, driver, memory and processing into separate virtual instances. First as shown in Figure 8, the isolation of the Wi-Fi driver into a separate virtual instance that reduces the risk exposure of the Wi-Fi driver to the EUD.

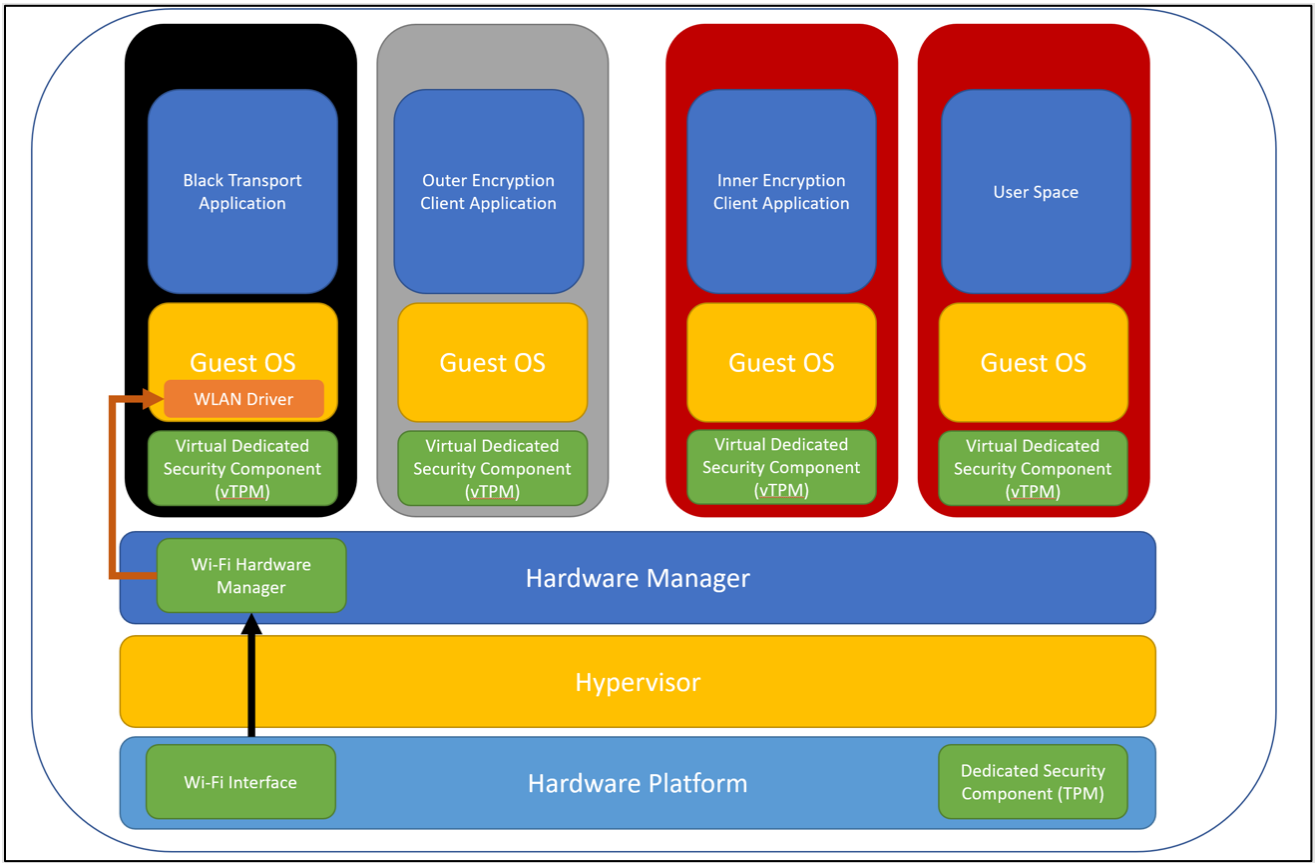


Figure 8. Virtualized EUD Wi-Fi Driver Isolation

Within the MA CP this allows for use of Wi-Fi to connect to a retransmission device instead of tethering the EUD physically. While in the CWLAN CP, this increases the security of the WLAN Client. The isolation additionally would provide separation to other functions of the EUD such as dedicated virtual instances for the Inner and Outer Encryption Clients, Black Network Transport and User Space.

7.1 Composed Virtualized EUDS

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

These isolated domains allow multiple parts of an EUD to be built securely into a single piece of hardware and ensure that separate IP stacks are used for each connection layer. The hypervisor provides the virtual networks that are used by the domains for internal network connections required for dual layers of encryption. Each isolated domain should include the following sub-domains:

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

2) Transport domain to connect to the Black Transport Network

3) Transport domain to connect to the Outer Encryption Component

4) Transport domain to connect to the Inner Encryption Component

End users should only be able to access end user domains, and other domains should be managed by an administrator. Additional domains can be added for device management functions.

A Mobile Access Virtual EUD must either be physically connected to a Black Transport Network or have a virtual OS dedicated to the Black Transport Network where all the wireless application run in that separate virtual environment. ACWLAN Virtual EUD has a virtual OS dedicated to the WLAN Client and as this WLAN client acts as the Outer Encryption layer. This OS must be chosen from the CSfC Components List for WLAN Clients and OSs. The IPsec Clients and TLS application must only run on an OS that was tested within the NIAP Target of Evaluation.

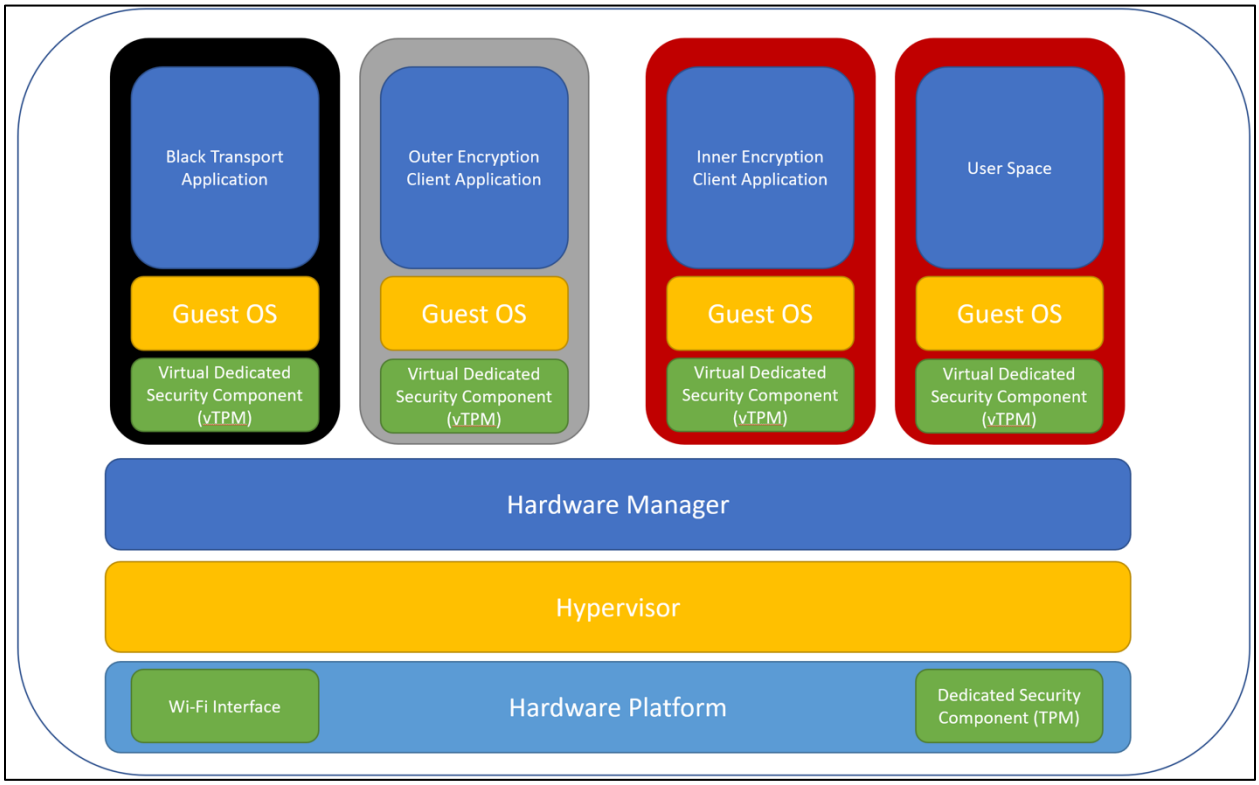


Figure 9. Mobile Access Virtualized EUD

A logical diagram of the components of the Virtualized EUD can be seen in Figure 9. The EUD itself runs on physical hardware chosen from the PP for GPOS. The hardware may integrate a DSC that is chosen from the Collaborative PP for DSC. The EUD's Hypervisor must be chosen from the Protection Profile for Virtualization and PP-Module for Client Virtualization. The EUD's OS must be chosen from the PP for GPOS. The WLAN Client must be chosen from PP-Module for WLAN Client and the guest OS on which it runs must be chosen from the Protection Profile for General Purpose Operating Systems. The VPN Client must be chosen from the PP-Module for VPN Client and must be running on the OS on which it was evaluated. The VPN Client TLS App must be chosen from any of the following PPs: Functional Package for TLS, PP-Module for VVoIP, or Extended Package for Email. It must also run on the OS on which it was evaluated. For encryption, the EUD must use an encryptor that is chosen from the Collaborative PP for

414 Full Drive Encryption – Authorization Acquisition and Collaborative PP for Full Drive Encryption -
415 Encryption Engine.

416 **Table 10. Virtual EUD Components**

Component	Protection Profile
EUD Hardware	*Protection Profile for General Purpose Computing Platform*
EUD- Dedicated Security Component (Optional)	*Collaborative Protection Profile for Dedicated Security Component*
Hypervisor	*Protection Profile for Virtualization* and *PP-Module for Client Virtualization*
WLAN Guest Operating System	*Protection Profile for General Purpose Operating Systems*
WLAN Client	*PP-Module for Wireless Local Area Network Client*
Outer VPN Client	*PP-Module for VPN Client*
Inner VPN Client	*PP-Module for VPN Client*
EUD Encryption	*Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*

417 ## 7.2 MDF VIRTUALIZED EUDS

418 MDF Virtualized EUDs are traditional MDF EUDs that run additional Type 1 Hypervisor. These isolated
419 domains allow multiple parts of an EUD to be built securely into a single piece of hardware and ensure
420 that separate IP stacks are used for each connection layer. The hypervisor provides the virtual networks
421 that are used by the domains for the internal network connections required for the dual layers of
422 encryption. Each isolated domain should include the following subdomains: 1) a user domain where the
423 user can interact with the EUD, 2) a transport domain to connect to the Black Transport Network, 3) a
424 transport domain to connect to the Outer Encryption Component, and 4) a transport domain to connect
425 to the Inner VPN Gateway. End users should only be able to access end user domains, and other
426 domains should be managed by an administrator. Additional domains can be added for device
427 management functions. Virtualized EUDs create virtual instance of both kernels and OSs use namespace
428 separation to abstract out applications and functionality of the EUD, such as IPsec Client, WLAN Client,
429 or TLS Client, into a separate name space and their own separate virtualized environment with little to
430 no resource sharing between the virtual environments.

431 A Mobile Access Virtual EUD must either be physically connected to a Black Transport Network or have a
432 virtual OS dedicated to the Black Transport Network where all the wireless applications run on that
433 separate virtual environment. This allows for MA CP EUDs to leverage the driver separation of the Type

1 Hypervisor to eliminate the requirement for a tethered retransmission device. While a Campus WLAN Virtual EUD has a virtual OS dedicated to the WLAN Access Client.

The EUD itself runs on physical hardware from the Protection Profile for MDF. The hardware may integrate a DSC that is chosen from the Collaborative Protection Profile for Dedicated Security Component. The EUD's Hypervisor must be chosen from the Protection Profile for Virtualization and PP-Module for Client Virtualization. The WLAN Client must be chosen from PP-Module for WLAN Client and the guest OS on which it runs must be chosen from the Protection Profile for GPOS. The VPN Client must be chosen from the PP-Module for VPN Client and must run on the OS on which it was evaluated. The VPN Client TLS App must be chosen from any of the following PPs: Functional Package for TLS, PP-Module for Voice and Video over IP (VVoIP), or Extended Package for Email. It must also run on the OS on which it was evaluated. For encryption, the EUD must use an encryptor chosen from the Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine.

Table 11. Virtual EUD Components

Component	Protection Profile
EUD Hardware	*Protection Profile for Mobile Device Fundamentals*
EUD-Dedicated Security Component (Optional)	*Collaborative Protection Profile for Dedicated Security Component*
Hypervisor	*Protection Profile for Virtualization* and *PP-Module for Client Virtualization*
WLAN Guest Operating System	*Protection Profile for Mobile Device Fundamentals*
WLAN Client	*Protection Profile for Mobile Device Fundamentals*
Outer VPN Client	*PP-Module for VPN Client*
Inner VPN Client	*PP-Module for VPN Client*
EUD Encryption	*Protection Profile for Mobile Device Fundamentals*

7.3 VM ARCHITECTURE

Within the Composed Virtualized EUDs there are several methods and architectures that may be used to create an EUD that meets the requirements of a Virtualized EUD. This addendum will not prescribe any particular architectures but instead present concepts and best practices that should be used in implementation of the Composed Virtualized EUDs. These concepts include:

- VM Interconnectivity
- Limited VMs
- Read Only VMs

These concepts and best practices additionally can be used when implementing a Software Separated EUD as described in Section 8.

7.3.1 VM Interconnectivity

The separation that the Type 1 hypervisor adds between the VMs must be considered when doing the interconnection between the VM for the data to make its way from the Black untrusted network to the Red user space. All VMs should have their connection limited to what is necessary for the VMs to function 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 out by the data type handles such as black, gray, and red. For example, there should be a separate virtual switch that handles the Black data, Gray data, Red data, and a dedicated switch to pass data between the Black Network and the Black VM. Figure 10 depicts Virtual EUDs with separate virtual switches allowing for communication between the VMs with each switch dedicated to the type of data transiting the switch.

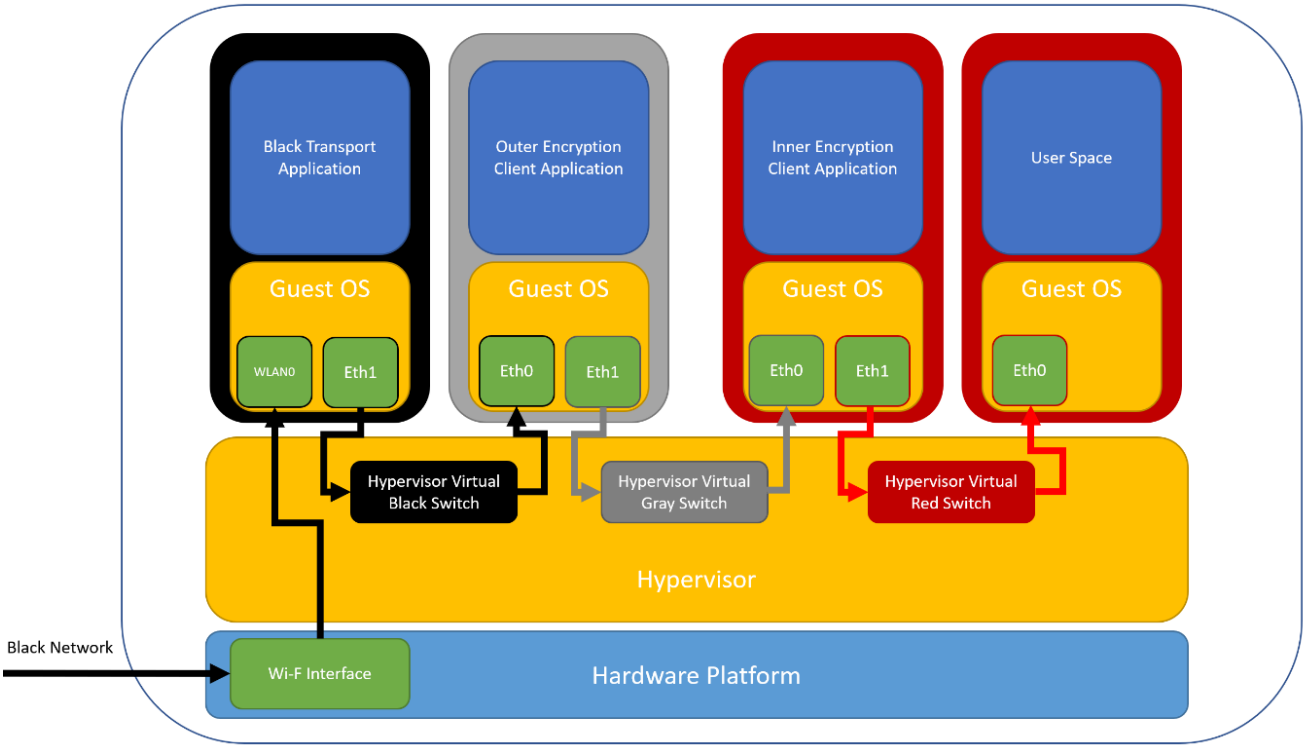


Figure 10. VM Interconnectivity

Another additional function that can be leveraged is for the VMs to run an independent firewall in 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.

7.3.2 LIMITED VMS

VM within a virtual EUD should be limited to only have the necessary core functions required for operation. All other additional functionality should be removed. An example of this is the Outer Encryption VM should only have the outer encryption client, network supplicants, firewall, and any additional supporting libraries and should have any non-essential functionality. Non-essential functionality can include user applications, text editors, and even user interfaces. These principals limited functionality should be applied to all VMs within a virtual EUD to further reduce the attack surface which each VM presents to the virtual EUD.

7.3.3 READ ONLY VMS

Within Virtualization technology is the concept of 'Read Only' VMs where the file system of the virtualized guest OS is in a 'read only' state. In this state, no changes to the guest OS's file system are permanent nor are the changes to these OSs persistent through rebooting the VMs. This guarantees that 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 very beneficial for VMs that handles the network functionality of the EUD. Additionally, this prevents any modification to the file system and reduces persistence through reboots. Within CSfC, this technology is not required to be deployed within a Virtualized EUD, but it is recommended that the Integrator consider technologies such as this to reduce the risk of operating the solution and improve the usability of the EUDs.

8 SOFTWARE SEPARATED COMPOSED EUDS

Software Separated EUDs is a category of technologies that offers some form of separation to a Composed EUD but does not meet the strict Type 1 Hypervisor requirements for a Composed Virtualized EUD. These technologies can include containerization, virtualization which does not conform with CSfC requirements for Virtualized EUDs in Section 7, and other software separation technologies. These currently do not have particular protection profiles written for them and thus cannot be tested for their exact functionality. Thus, all these software separation technologies must be tested against the GPOS PP and the security features of these technologies above those within GPOS will not be considered on an architectural level for CSfC solution but may be considered for individual solution deployments

8.1 CONTAINERIZED EUDS

Containerized EUDs use namespace separation to abstract out applications and functionality of the EUD, such as an IPsec Client, WLAN Client, or TLS App, into a separate namespace. Depending on its configuration, the Containerized EUD can either be used with a Mobile Access or Campus WLAN solution. Furthermore, different applications may be containerized to act as Black Transport, Outer Encryption and Inner Encryption. The EUD may containerize the WLAN Client for accessing a Black Transport Network that is not part of the two layers of encryption but is necessary for the connectivity of the EUD. The Outer Encryption of the EUD must be either a containerized WLAN Client or a containerized IPsec Client for connecting to the Outer Encryption Component. The Inner Encryption of the EUD must be either a containerized TLS Client or a containerized IPsec Client for connecting to the Inner Encryption Component.

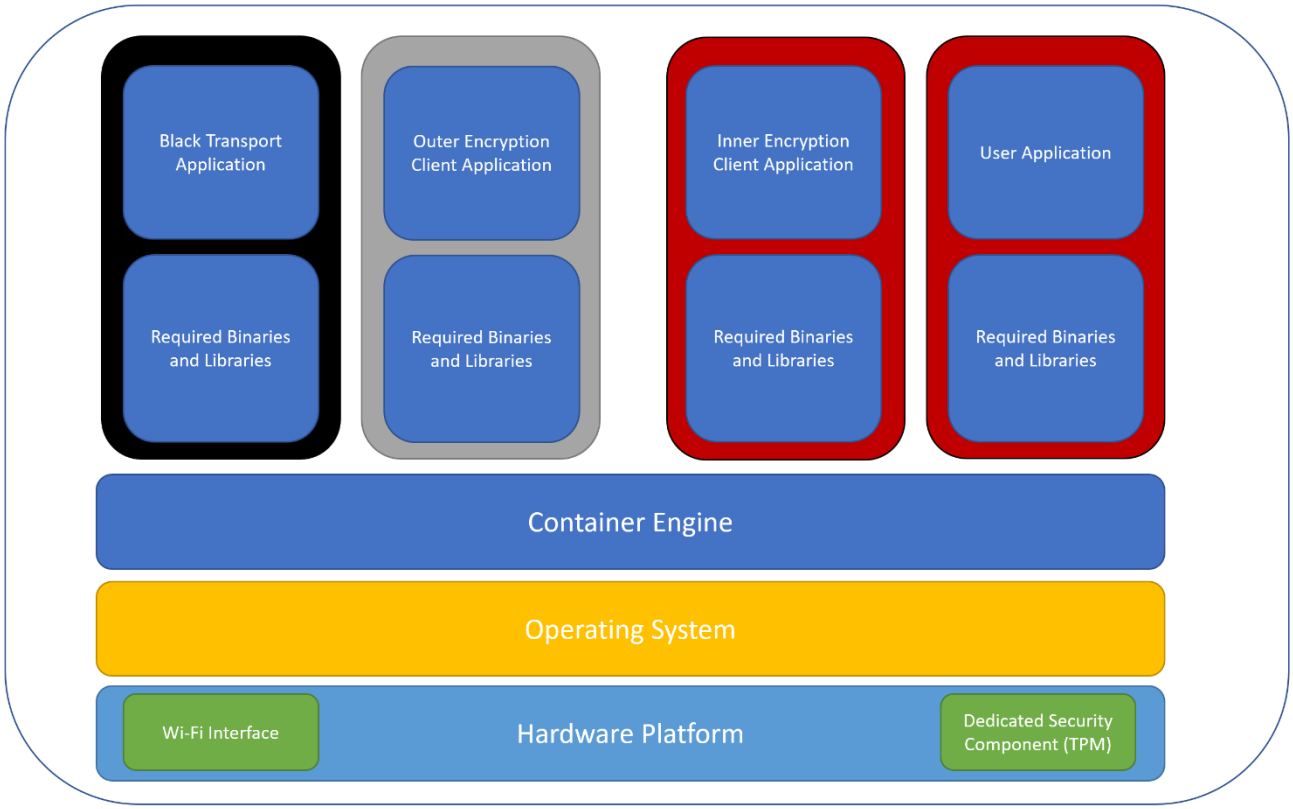


Figure 11. Mobile Access Containerized EUD

Figure 11 shows a logical diagram of the components of the Containerized EUD for a Mobile Access Solution. The EUD itself runs on physical hardware from the PP for General Purpose Computing Platform. The hardware may integrate a DSC chosen from the Collaborative PP for DSC. The EUD's OS must be chosen from the Protection Profile for GPOS. The containerization application software is located on the EUD's OS and includes all containerized applications. The WLAN Client must be chosen from PP-Module for WLAN Client, and it must be tested on the EUD's OS. The VPN Client must be chosen from the PP-Module for VPN Client, but it does not need to be tested on the EUD's OS. The TLS App must be chosen from any of the following PPs: Functional Package for TLS, PP-Module for Voice and Video over IP (VVoIP), or Extended Package for Email Clients. It also does not need to be tested on the EUD's OS. For encryption, the EUD must use an encryptor that is chosen from the Collaborative PP for Full Drive Encryption – Authorization Acquisition and Collaborative PP for Full Drive Encryption - Encryption Engine.

Table 12. Software Separated EUD Components

Component	Protection Profile
EUD Hardware	*Protection Profile for General Purpose Computing Platform*
EUD-Dedicated Security Component (Optional)	*Collaborative Protection Profile for Dedicated Security Component*

Host Operating System	*Protection Profile for General Purpose Operating Systems*
WLAN Client	*PP-Module for Wireless Local Area Network Client*
Outer VPN Client	*PP-Module for VPN Client*
Inner VPN Client	*PP-Module for VPN Client*
Inner TLS Application	*Protection Profile for Application Software and, Functional Package for TLS* or *PP-Module for Voice and Video over IP (VVoIP)* or *Extended Package for Email Clients*
EUD Encryption	*Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*

8.2 VIRTUAL EUDS

The Virtual Composed EUD is very similar to the Virtualized Composed EUD with the main exception that the virtualization engine is not a validated NIAP component and listed on the CSfC Components list. This could be because they are Type 1 Hypervisors which do not meet the separation requirements, or another form of virtualization such as a Type 2 Hypervisor where the virtualization engine runs on the existing EUD's OS. In these cases, the Hypervisor or operating system with the virtualization engine must be an OS from the CSfC Components List. All other requirements other than this are the same as detailed in Section 7.

8.3 SOFTWARE SEPARATED EUDS

The Software Separated EUD is a catch all for other separation technology that does not fit into either virtualization or containerization such as separation. These tend to be highly customized systems that are hard to categorize and generalize about them. These currently do not have particular protection profiles written for them and thus cannot be tested for their exact functionality. Thus, all these software separation technologies must be tested against the GPOS PP and the security features of these technologies above those in GPOS will not be considered on an architectural level for CSfC solution but may be considered for individual solution deployment.

9 DAR EUDS

The DAR CP has been used to provide an additional layer of security to CSfC DiT EUDs ensuring that their data is secure when powered off. As virtualization, containerization and security separation kernel technology become more prevalent with CSfC DiT solutions guidance on how DAR and their newer technologies must be given. The following section details how a Composed EUD interacts with the DAR CP.

Within a Composed EUD concept the validation of the OS, Hypervisor, and physical hardware of the EUD are core to the security of these devices. Within the DAR CP it is highly recommended that the OS and Hypervisor are from the CSfC Components list but not the hardware platform. The reason is the DAR components may rely upon the OS functions to perform various security services and ensure that the data is properly contain within the virtual machine.

9.1 DAR Virtual EUDs

As virtualization, containerization and security separation kernel technology becomes more prevalent within CSfC DiT solutions, it is necessary to provide guidance on how these Virtual EUDs must be treated within the DAR CP. The DAR CP's most vital role is to protect the confidentiality of the Red Data being stored and processed on the EUD. Thus, the User VM or space which stores and processes this Red Data must be protected with two layers of approved DAR encryption. The encryption that DAR uses, provides additional integrity to the operating system components further enhancing the security of the EUD and ensures that unauthorized changes have not been made to the core operating system components.

The methods of allowed Outer Encryption and Inner Encryption are listed below and further expanded later in this section:

Table 13. DAR Solution Design Summary

Outer Encryption	Inner Encryption	Inner Encryption Location	VM Suspension Allowed	Description	Related Figure
HWFDE	HWFDE	After Outer HWFDE	Yes	Double layer of HWFDE encryption covering the hypervisor, all VMs and software subcomponents	
HWFDE	SWFDE	After Outer HWFDE	Yes	A layer of HWFDE followed immediately by a layer of SWFDE encryption covering the hypervisor, all VMs and software subcomponents	Figure 12
HWFDE/SWFDE	FE	Encrypting the Red Data VM image	No	A single layer of HWFDE/SWFDE covering the Hypervisor, all VMs and software subcomponents followed by a FE encrypting the Red Data VM Image	Figure 13

Outer Encryption	Inner Encryption	Inner Encryption Location	VM Suspension Allowed	Description	Related Figure
HWFDE/SWFDE	SWFDE	Deployed on the Red Data VM	No	A single layer of HWFDE/SWFDE covering the Hypervisor, all VMs and software subcomponents followed by a SWFDE deployed on the Red Data VM	Figure 14
HWFDE/SWFDE	FE	Deployed on the Red Data VM	No	A single layer of HWFDE/SWFDE covering the Hypervisor, all VMs and software subcomponents followed by a FE deployed on the Red Data VM	Figure 15

As seen in figure 12, the outer layer of encryption that a virtual EUD must implement must encompass the entire EUD by using either SWFDE or HWFDE. This encryption must include encrypting the Hypervisor or Virtualization technologies and further encrypting all files and VMs used by them. This encryption will both provide the first layer of protection to the Red Data and provide integrity protection to all software components making up the EUD.

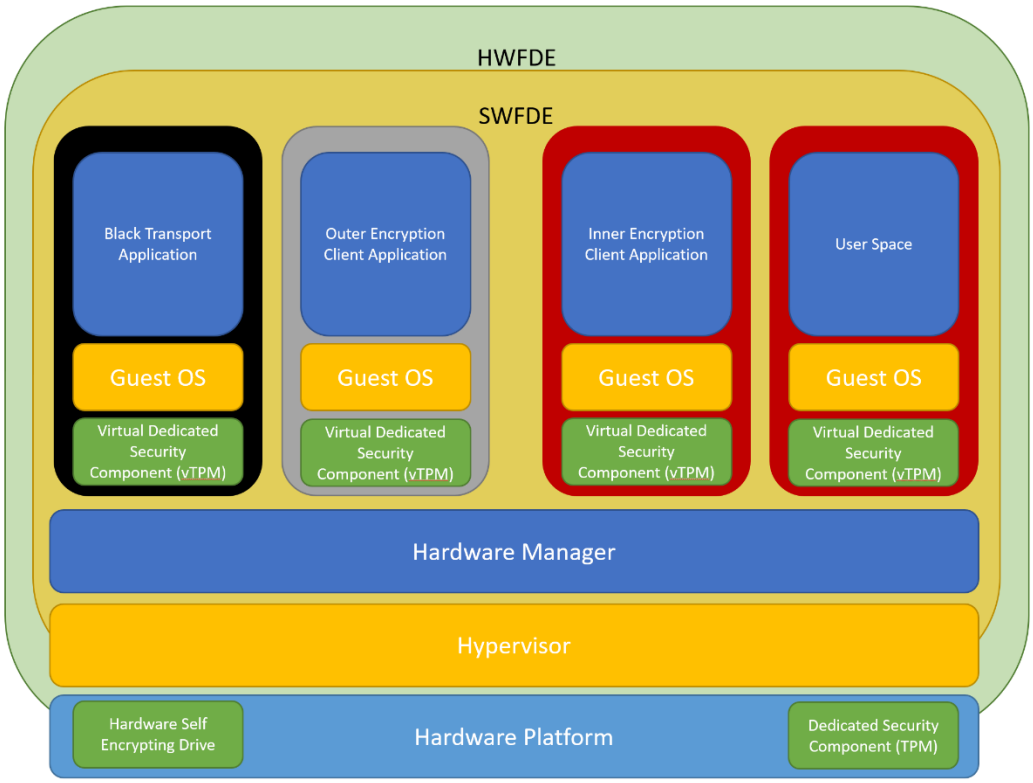
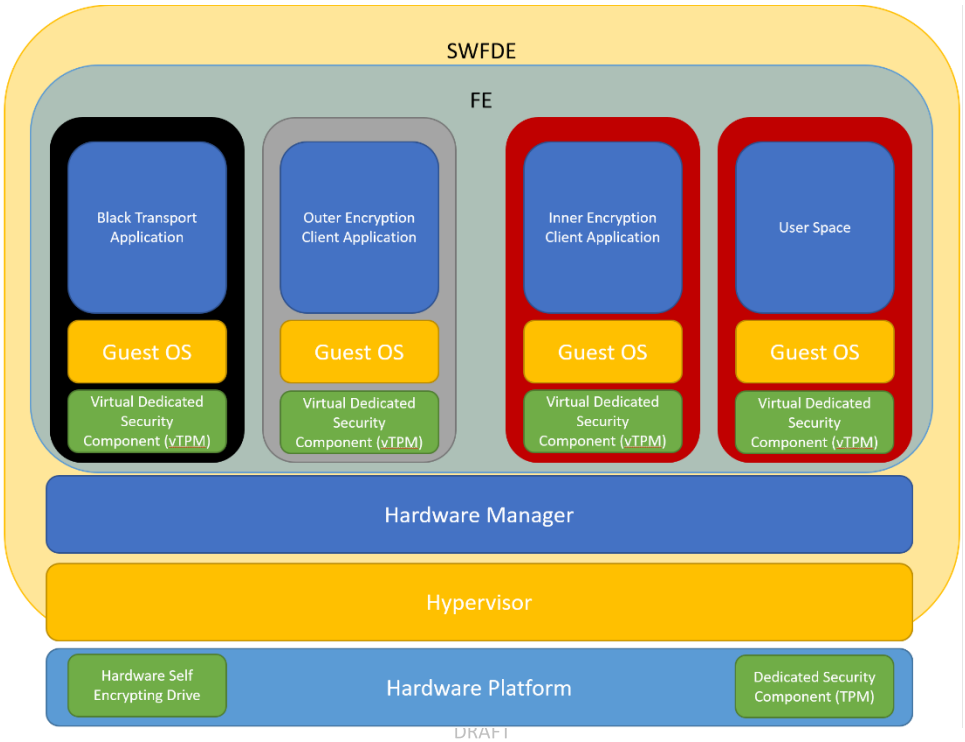


Figure 12. Virtualized DAR EUD with HWFDE and SWFDE

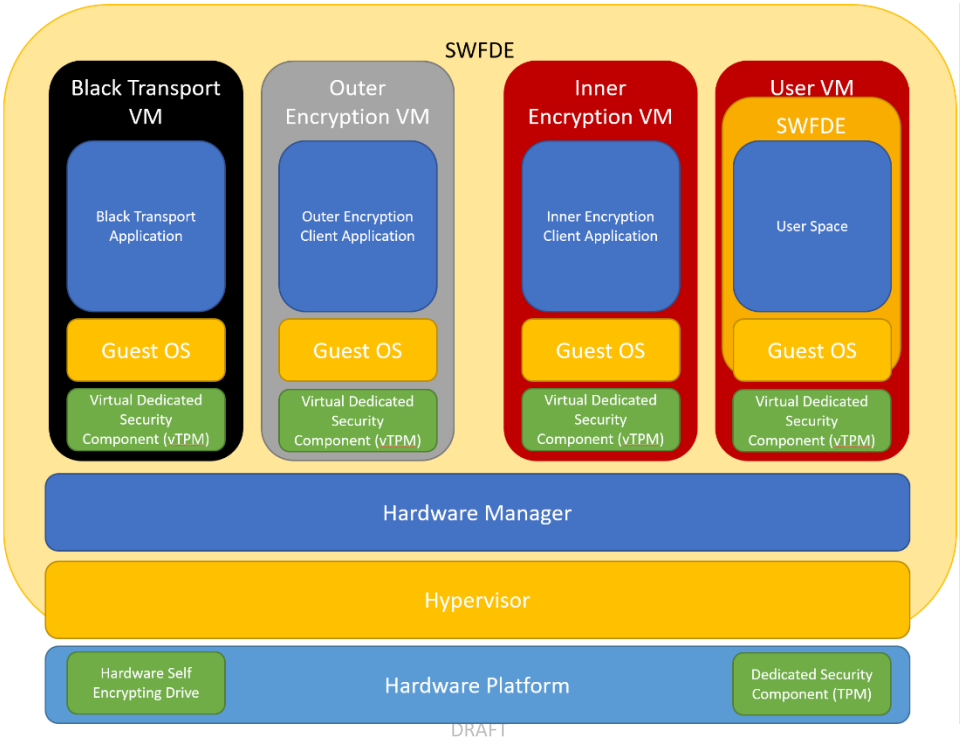
As seen in figure 13, the inner layer of encryption used to protect the confidentiality of the Red Data can provide additional integrity to the other components of the Virtual EUD. It is preferred that the inner layer of encryption be a SWFDE HWFDE layer of encryption immediately following the outer layer of encryption, as shown in Figure 11, to provide the maximum amount of confidentiality and integrity to all components of the virtual EUD. This method of encryption in virtual EUD is not practical or possible in all use cases thus additional methods of inner encryption are allowed which focus on protecting the Red Data.



582

583 **Figure 13. Virtualized DAR EUD with SWFDE and FE**

584 As in Figure 12, the first of these methods for an inner layer of encryption is to have a File Encryptor
585 encrypt the VM's images and any additional file locations where information on these VMs are stored.
586 Though it is not required it is highly recommended that the other VMs be encrypted as well Inner
587 Encryption Client VM. This method requires the File Encryptor to integrate with the hypervisor to run or
588 to integrate with the underlying Hypervisor OS.



589

590 **Figure 14. Virtualized DAR EUD with SWFDE and VM Based SWFDE**

591 Another method for inner encryption is to implement the inner layer of encryption onto the VM
592 handling the Red Data using a SWFDE. This would provide excellent protection to the Red Data VM
593 before being powered on and offer a familiar user experience. In this method there are concerns about
594 suspension and VM backup technologies since they save the state of VMs that normally includes
595 processor caches, memory, and other critical system information outside of the VM where it is not
596 protected by the inner layer of DAR. Thus, VM suspension and backup technologies cannot be used
597 when doing this method of DAR on Virtualized EUDs. It is not required but it is recommended that the
598 other VMs have their native platform encryption enabled as well.

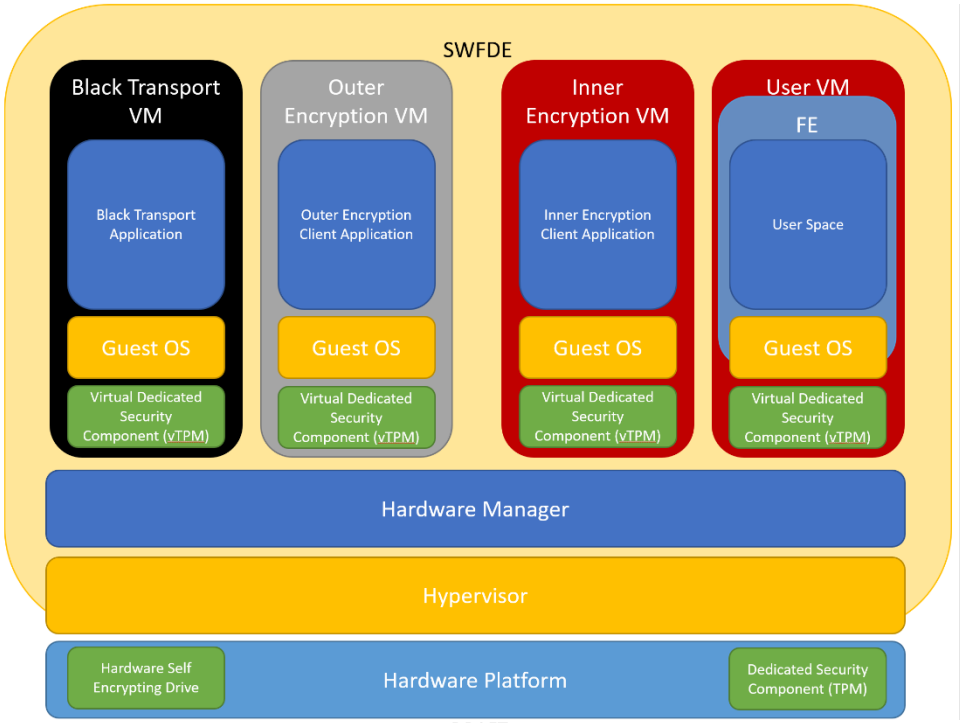


Figure 15. Virtualized DAR EUD with SWFDE and VM Based FE

The final method of accomplishing the inner encryption is to implement the inner layer of encryption onto the VM handling the Red Data using a File Encryptor. This would provide protection to the Red Data file system and protect the confidentially of the Red Data. In this method there are concerns about suspension and VM backup technologies since they save the state of VMs which normally includes processor caches, memory, and other critical system information outside of the VM where it is not protected by the inner layer of DAR. Thus, VM suspension and backup technologies cannot be used when doing this method of DAR on Virtualized EUDs. It is not required but recommended that the other VMs have their native platform encryption enabled as well.

9.2 DAR EUDs Other Security Features

There are additional design features that affect the security of deploying DAR on a Virtual EUD. These features include the usage of Platform Encryption (PE) within the virtual architecture. Second the use and security concerns involving VM suspension and VM Backups. Finally, the use of both Virtual DSC and hardware back DSC.

9.2.1 VM Platform Encryption

Platform encryption, also referred to as platform DAR, is provided by the OS for platform-wide data encryption, transparently encrypting sensitive user data. The platform encryption layer requires hardware-backed secure key storage, with the goal of reducing the need for long and complex passwords. Typically, PE is used only as the outer layer of encryption but by leveraging virtualization technologies it is possible to use platform encryption as the inner layer of encryption after an already existing SWFDE or HWFDE.

OSs typically have a built-in platform encryption within them some of which are not listed on the CSfC Components List. Though they are not listed components they can still offer additional security to a EUD's VMs not handling Red Data. By enabling the platform encryption on the VM not handling Red Data, it further protects the confidentiality and integrity of these VMs by protecting any key material, configurations and preventing any changes to these VMs. This PE can be tied into a virtual DSC to allow for these VMs to decrypt and boot automatically without user interaction.

9.2.2 VM Suspension and Backup

Virtualization technologies have several methods of saving the running state of the actively running VM these include suspension and backup. Suspending a VM normally entails the user pausing operation on the VM where its state is saved and can be safely powered off and brought back up in the same state later. Backing up a VM works in a similar manor where the state is saved and the VM can be restored to that previous state later. These technologies work by saving the processor state, cache, active memory and a disk image of the VM. These technologies when combined with PE or FE running on the Red Data VM pose a security risk to the Red Data. Since the PE and FE are solely based on the OS running in the Red VM and the suspension and backup features operate at the hypervisor level. It is possible for the hypervisor to suspend the VM in a decrypted state or save a decrypted image of the VM where it is only encrypted once. Thus, when relying on any DAR solution that does not encrypt the hypervisor twice all forms of VM Suspension and Backup must be disabled.

9.2.3 DAR DSC

A DSC such as a TPM can provide an invaluable asset to a DAR EUD providing a degree of validation into the hardware of the EUD and more importantly supplying a secure storage area for key material. This storage area should be used to store any keys that are used in the decryption of the DAR EUD's encryption layers. The additional signing validation of drivers and such security related functions are greatly beneficial to the DAR EUD as a whole and these functions can be further pushed into a Virtual DAR EUD. By relying on the hypervisor to have virtualization technology allowing for TPM functionality to be pushed into the VM itself through Virtual Trusted Platform (vTPM) technologies these same benefits can be used for the VM within. These benefits could include system level checks before booting, key generation, secure key storage and automated decryption of platform encryption for non-DAR protected VMs.

9.3 DAR EUD Requirements

This details the requirements that will be added to the DAR CP as part of the EUD Composition Update in DAR CP 5.1.

9.3.1 DAR Product Selections Requirements

The following table is a list of DAR CP product selection requirements that will be appended or changed as part of the EUD Composition Update.

659 **Table 14. DAR Production Selection Requirements**

Req #	Requirement Description	Solution Designs	Use Case	Threshold / Objective	Alternative
DAR-PS-8	The EUD's Operating System used must be chosen from the list of Operating Systems on the CSfC Components List.	HF, HS, SF, HH	HF, HS, SF, HH	O	DAR-PS-10 or DAR-PS-11
DAR-PS-10	Products used for Mobile Platform EUDs must be chosen from the list of Mobile Platforms on the CSfC Components List.	HF, HS, SF, HH	HF, HS, SF, HH	O	DAR-PS-9 or DAR-PS-11
DAR-PS-11	The EUD's Hypervisor used must be chosen from the list of Client Hypervisors on the CSfC Components List.	HF, HS, SF, HH	HF, HS, SF, HH	O	DAR-PS-9 or DAR-PS-10
DAR-PS-12	The EUD must have a Dedicated Security Component chosen from the list of Dedicated Security Components on the CSfC Components List.	HF, HS, SF, HH	HF, HS, SF, HH	O	Optional

660 ### 9.3.2 DAR EUD REQUIREMENT

661 The following table lists DAR CP requirements that will be appended or changed as part of the EUD
662 Composition Update.

663 **Table 15. DAR EUD Requirements**

Req #	Requirement Description	Solution Designs	Use Case	Threshold / Objective	Alternative
DAR-EU-40	If virtualization technologies are used within the EUD and the Inner Layer of Encryption is inside the Red Data VM, VM suspension and VM backup technology must be disabled or disallowed on the Red Data VM.	HF, HS, SF, HH	HF, HS, SF, HH	T=O	

664 # 10 HARDWARE SEPARATED EUDS

665 Within the CSfC architecture, especially the MA CP, there is the concept of multiple components making
666 up a single EUD. This concept is exemplified by the retransmission device (RD) and the Dedicated Outer
667 VPNs which can be paired with a traditional EUD. This is done to pass along functionality that causes risk
668 to a separate component other than the EUD handling red data or having the separate hardware
669 perform a function that the EUD is incapable of performing. This concept can be expanded on to further
670 enhance the security of an EUD or allow for EUDs which cannot meet the requirements placed on
671 traditional EUDs such as a laptop, smartphone, tablet, or computer.

672 The concept of multiple EUD components will expand to include both a Dedicated Inner VPN and a Red
673 Compute Hardware. This allows for EUDs that cannot operate the Inner Encryption to still be used with
674 CSfC or to pass along the risk from the Red Compute to the other dedicated component. The Dedicated

Inner and Red Compute Hardware are objective design features within a CSfC Solution and are not required to be implemented by the customer.

10.1 Retransmission Devices (Black Transport Component)

An RD is a government owned device dedicated to be a pass through between the EUD and untrusted Black Network. The RD has two important functions; first to separate out the wireless transport from the EUD and secondly, to provide a separation point between the EUD and an untrusted Black Network. The ideal form of an RD would be a firewall that has the proper transport method between it and the Black Networks. Devices such as Wi-Fi Hotspots, smartphone sleeves, and Mobile Routers are the most common RDs. On its external interface, an RD can be connected to any type of medium (e.g., Cellular, Wi-Fi, SATCOM, Ethernet) to gain access to the black network. While on the internal interface the RD must use either Ethernet cable or Wi-Fi. The option for Wi-Fi connection is only available for Virtualized EUD as described in Section 7. There are no selector requirements for an RD but instead, an objective requirement to be chosen from the CSfC Components list for firewalls. Additionally, there are functional security requirements described within the MA CP.

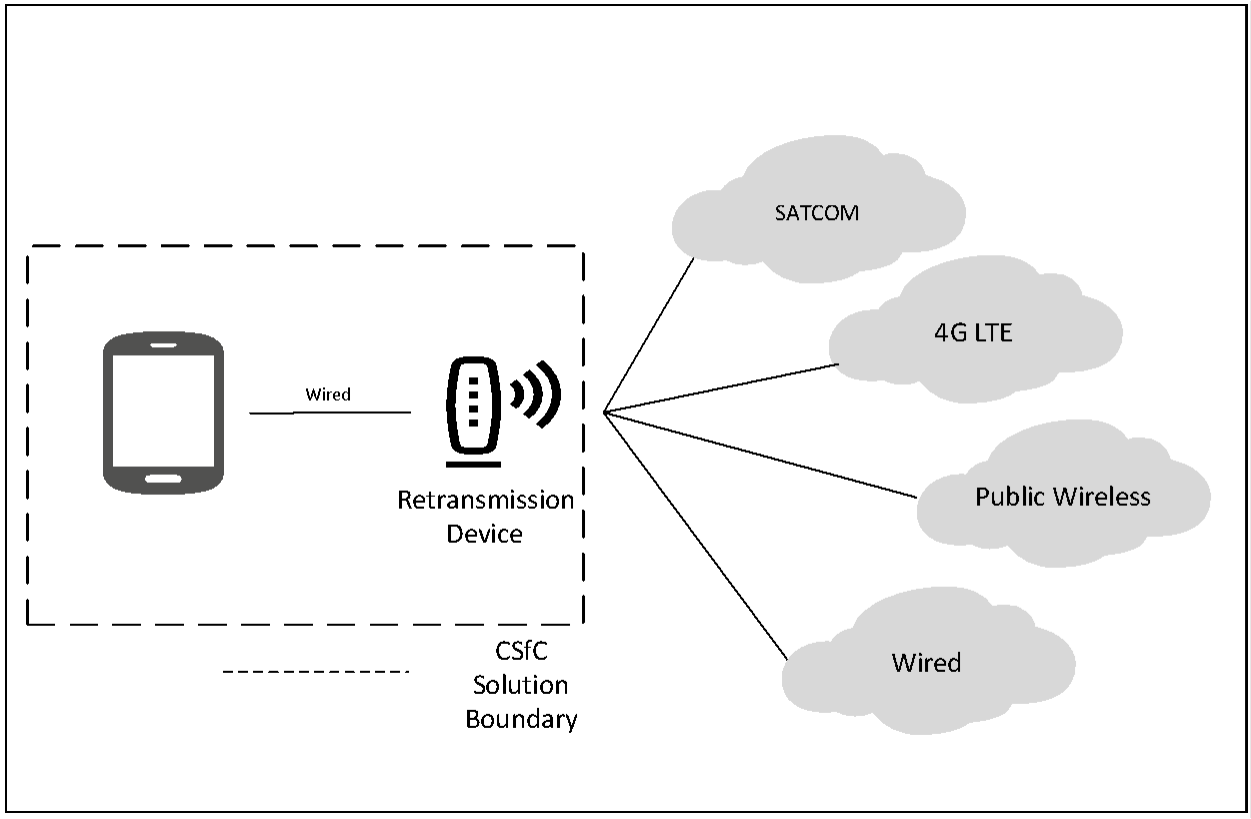


Figure 16. MA CP Retransmission Device

10.2 Dedicated Outer VPN (Outer Encryption Component)

A Dedicated Outer VPN is a separate component that can be used as the Outer VPN for an EUD. These Dedicated Outers normally are small travel routers or similar network gear. Another option for a Dedicated Outer VPN is to have it be a Composed EUD as described in Section 6. The Dedicated Outer

VPN included as part of the EUD must be physically connected to the computing platform using a wired connection preferably an Ethernet cable.

For the first option with the Dedicated Outer VPN being a travel router or other similar component, the Dedicated Outer VPN is selected from either the *IPsec VPN Gateway* section or the *IPsec VPN Client* 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.

When the Dedicated Outer VPN is a composed EUD the OS is selected from the *OS* section of the CSfC Components List. The Dedicated Outer VPN hardware is selected from the *Hardware Platform* section of the CSfC Components List. The Dedicated Outer VPN hardware is selected from the *Hardware Platform* section of the CSfC Components List. Finally, the Dedicated Outer VPN's VPN is selected from the *IPsec VPN Client* section of the CSfC Components List.

10.2.1 DEDICATED OUTER WLAN (OUTER WIRELESS ACCESS)

The Dedicated Outer VPN is a concept which currently exists only within the MA CP, this addendum proposed to expand the use of this component to allow for CWLAN CP to benefit from the same hardware separation which MA CP. This would a dedicated component which handles the Wi-Fi connectivity for a EUD which is either incapable of operating a Wi-Fi connection or to pass along the risk of a Wi-Fi connection to another separate component. These Dedicated Outers normally are small travel routers, Wi-Fi Access Point or similar network gear. Another option for a Dedicated Outer WLAN to have it be a Composed EUD as described in Section 6. The Dedicated Outer WLAN included as part of the EUD must be physically connected to the computing platform using a wired connection preferably an Ethernet cable.

For the first option with the Dedicated Outer WLAN being a travel router, Wi-Fi Access Point or other similar component, the Dedicated Outer WLAN is selected from either the WLAN Access System section or the WLAN *Client* section of the CSfC Components List. When a Dedicated Outer WLAN is included as part of an EUD, it provides configuration and enforcement of network packet handling rules for the Outer layer of encryption.

When the Dedicated Outer WLAN is a composed EUD the OS is selected from the *OS* section of the CSfC Components List. The Dedicated Outer WLAN hardware is selected from the *Hardware Platform* section of the CSfC Components List. The Dedicated Outer WLAN hardware is selected from the *Hardware Platform* section of the CSfC Components List. Finally, the Dedicated Outer WLAN's OS is selected from the the WLAN Clients section of the CSfC Components List.

10.2.1.1 Campus WLAN Dedicated Outer WLAN Requirements

The following table lists the product selection requirements that will be appended or changed to the CWLAN CP as part of the EUD Composition Update.

734 **Table 16. Campus WLAN Production Selection Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PS-21	If the solution uses a Dedicated Outer Wi-Fi as part of an EUD, it must be chosen from the list of WLAN Access Systems or WLAN Clients on the CSfC Components List.	T=O	WLAN-PS-3

735

736 The following table lists the requirements that will be appended or changed to the CWLAN CP as part of
737 the EUD Composition Update for Dedicated Outer WLAN.

738 **Table 17. Campus WLAN Dedicated Outer WLAN Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WO-1	If a Dedicated Outer WLAN is used it must be dedicated to a single security level and only provide the Outer layer of Wi-Fi to Computing Devices connecting to a Red Network of the same security level.	T=O	
WLAN-WO-2	A Computing Device must only connect to a Dedicated Outer WLAN authorized as part of the WLAN CP solution.	T=O	
WLAN-WO-3	The Dedicated Outer WLAN must comply with all requirements in Tables 9.	T=O	
WLAN-WO-4	If a Dedicated Outer WLAN is used, all EUDs must connect to Dedicated Outer WLAN devices with a wired connection.	T=O	
WLAN-WO-5	If a Dedicated Outer WLAN is used Wi-Fi must be disabled on the EUD.	T=O	

739

740 ## 10.3 Dedicated Inner VPN (Inner Encryption Component)

741 A Dedicated Inner VPN is a separate component that can be used as the Inner VPN for an EUD.
742 Additionally Dedicated Outer VPN is required when a Dedicated Inner VPN is used. These Dedicated
743 Inner VPNs normally are small travel routers or similar network gear. Another option for a Dedicated
744 Outer VPN is to have it be a Composed EUD as described in Section 6. The Dedicated Inner VPN included
745 as part of the EUD must be physically connected to the computing platform using a wired connection
746 preferably an Ethernet cable. A Dedicated Outer and Dedicated Inner may be combined into the same
747 hardware, though for this use case it is preferred to have these to be separate components.

748 For the first option with the Dedicated Inner VPN being a travel router or other similar component, the
749 Dedicated Inner VPN is selected from either the *IPsec VPN Gateway* section or the *IPsec VPN Client*
750 section of the CSfC Components List. When a Dedicated Inner VPN is included as part of an EUD, it
751 provides configuration and enforcement of network packet handling rules for the Inner layer of
752 encryption. The configuration settings of the Dedicated Inner VPN may need to be updated when
753 entering new environments (e.g., updating the Default Gateway). Dedicated Inner VPNs are dedicated

to a single security level and can only provide the Inner layer of IPsec for clients connecting to a Red Network of the same security level.

When the Dedicated Inner VPN is a composed EUD the OS is selected from the *OS* section of the CSfC Components List. The Dedicated Inner VPN hardware is selected from the *Hardware Platform* section of the CSfC Components List. The Dedicated Inner VPN hardware is selected from the *Hardware Platform* section of the CSfC Components List. Finally, the Dedicated Inner VPN's VPN is selected from the the *IPsec VPN Client* section of the CSfC Components List.

10.4 Red Compute Hardware

The Red Compute Hardware is a dedicated Red Component whose role is to only handle the classified information and not to handle any of the encryption required to connect to a CSfC Solution. This dedicated Red Compute is expected to be Smartphone, Tablet, Laptop, or other standard EUD but may additionally be a non-traditional compute platform which does not fit in the concept of EUDs. The Red Compute must be physically connected to the Dedicated Inner VPN using a wired connection preferably an Ethernet cable.

The Red Compute Hardware must either be a Composed EUD or an MDF EUD. When the Dedicated Inner VPN is a composed EUD the Operating System is selected from the *Operating System* section of the CSfC Components List. The Dedicated Inner VPN hardware is selected from the *Hardware Platform* section of the CSfC Components List.

11 ACCESS CROSS DOMAIN SOLUTION EUDS

As the use of EUD based Access Cross Domain Solutions within CSfC Solutions becomes more common, uniform guidance on how they may be deployed as CSfC EUDs. Access CDSs are a type of CDS that provides access to a computing platform, application, or data residing on different security domains from a single device without any transfer between the various domains. Access CDSs are used within CSfC solutions to fully replace a traditional EUD. Thus, the National Cross Domain Strategy Management Office (NCDSMO) and the CSfC Program have partnered together to provide this guidance. The specific CDS targeted here are Access CDSs that rely of virtualization technologies for separation of different domains. These Access CDSs must go through a validation process and then it may be listed on the CDS Baseline. For any additional information on CDS contact the NCDSMO at ncdsmo@nsa.gov or local CDS support element.

Reciprocity between the NCDSMO Baseline and the CSfC Components List allows for the NCDSMO Baseline to be equivalent to the GPCP PP and Virtualization Client Module. All Access CDSs will not be automatically allowed to act as a CSfC EUD, they will only be allowed on a case-by-case basis based on input on the CSfC program and the NCDSMO. To allow for an Access CDS to be used within a CSfC Solution contact the CSfC Program Management Office (PMO), csfc@nsa.gov, to discuss the requirements and necessary information to allow for an Access CDS within CSfC Solutions.

Table 18. Virtual EUD Components

Component	Protection Profile
EUD	CDS Baseline listed Access CDS

EUD-Dedicated Security Component (Optional)	*Collaborative Protection Profile for Dedicated Security Component*
Hypervisor	CDS Baseline listed Access CDS
WLAN Guest Operating System	*Protection Profile for General Purpose Operating Systems*
WLAN Client	*PP-Module for Wireless Local Area Network Client*
Outer VPN Client	*PP-Module for VPN Client*
Inner VPN Client	*PP-Module for VPN Client*
EUD Encryption	*Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition and Collaborative Protection Profile for Full Drive Encryption - Encryption Engine*

The customer must ensure they use a current NCDSMO baseline CDS and that it is maintained in accordance with NCDSMO requirements. The security related components of the CDS must be maintained as directed by the NCDSMO such as the Hypervisor and EUD Encryption. There are other components which in additional to NCDSMO requirements they must comply with CSfC Program requirements. These include VPN Client, TLS Client, SRTP Client and WLAN Client. The VPN Client, TLS Client, SRTP Client, WLAN Client and security relevant updates for the Guest Operating Systems are expected and required to be updated as part of the CSfC Components lifecycle and updating them will not affect the status of these devices on the CDS Baseline. For questions or conflicting guidance on this guidance contact the CSfC PMO at csfc@nsa.gov.

APPENDIX A. GLOSSARY OF TERMS

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).

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.

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.

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.

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)

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

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

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).

Platform Certificate - A Trusted Computing Group (TCG) defined X.509 Attribute Certificate that asserts the platform's security properties and configuration as shipped.

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.

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

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.

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

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

TLS Client – A component on a TLS EUD that can provide the Inner layer of data in transit encryption.

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

Virtual EUD – An EUD that contains at least four virtual machines (End User Domain, Inner Encryption domain, Outer Encryption Domain and a Black Transport Domain) as described in section 6.3.1

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	Meaning
BIOS	Basic Input/Output System
CDS	Cross Domain Solution
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CP	Capability Package
cPP	Collaborative Protection Profile
CSD	Cybersecurity Directorate
CSfC	Commercial Solutions for Classified
CWLAN	Campus Wireless Local Area Network
DAR	Data-At-Rest
DiT	Data-in-Transit
DoD	Department of Defense
DSC	Dedicated Security Component
EUD	End User Device
FIPS	Federal Information Processing Standards
FDE	Full Disk Encryption
GPCP	General Purpose Compute Platform
GPOS	General Purpose Operating System
GSM	Hardware Security Modules
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HWFDE	Hardware Full Disk Encryption
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
MA	Mobile Access
MDF	Mobile Device Fundamentals
NCDSMO	National Cross Domain Strategy Management Office
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
O	Objective
OS	Operating System
PE	Platform Encryption
PMO	Program Management Office
PP	Protection Profile
RD	Retransmission Device
RFC	Request for Comment
RSA	Rivest Shamir Adelman algorithm
SAs	Security Administrators

Acronym	Meaning
SDE	Secure Data Element
SDO	Security Data Objects
SE	Secure Elements
SEP	Secure Enclave Processor
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Manager
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
SWFDE	Software Full Disk Encryption
T	Threshold
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEFI	Universal Extensible Firmware Interface
VoIP	Voice over Internet Protocol
VVoIP	Voice and Video over IP
VM	Virtual Machine
VPN	Virtual Private Network
vTPM	Virtual Trusted Platform Module
WLAN	Wireless Local Area Network
WPA3	Wi-Fi Protected Access 3

865

APPENDIX C. REFERENCES

Document	Title	Date
CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2015
CNSSP 15	*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*	October 2016
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	November 2021
DoDI 8420.01	*Commercial Wireless Local-Area Network Devices, Systems, and Technologies.* Office of the CIO of the DOD	November 2017
DoDI 8540.01	Department of Defense Instruction 8540.01: *Cross Domain Policy*	August 2017
FIPS 140-3	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf	March 2019
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	August 2015
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 201-2	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	August 2013
IPsec VPN Client PP 2.1	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*. https://niap-ccevs.org/MMO/PP/mod_vpn_cli_v2.1.pdf	October 2017
ISO 9594-8	*Public-Key and Attribute Certificate Frameworks*	May 2017
NSA Suite B	*NSA Guidance on Suite B Cryptography (including the Secure Sharing Suite (S3))*. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004

Document	Title	Date
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman	December 2005
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5288	*IETF RFC 5288 AES Galois Counter Mode (GCM) Cipher Suite2 for TLS*. J. Salowey, A. Choudhury, D. McGrew	August 2008
RFC 5289	*IETF RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*. E. Rescorla	August 2008
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
RFC 7296	*Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen	October 2014

Document	Title	Date
RFC 8422	*Elliptic Curve Cryptography (ECC) Cypher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*. Y. Nir, S. Josefsson, M. Pegourie-Gonnard	August 2018
RFC 8446	*The Transport Layer Security (TLS) Protocol Version 1.3*. E. Rescorla	August 2018
RFC 8603	*Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile*. M. Jenkins, L. Zieglar	May 2019
SP 800-37	*Risk Management Framework for Information Systems and Organizations.* Joint Task Force	April 2021
SP 800-53	*NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	September 2020
SP 800-56A	*NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	April 2018
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	March 2019
SP 800-56C	*NIST Special Publication 800-56C Rev 2, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	August 2020
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	March 2019
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et al.	April 2011
RFC 7714	*AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP). D. McGrew*	December 2015
	TCG Platform Certificate Profile, Version 1.1 Revision 15	February 2019
	Trusted Computing Group, TCG PC Client Reference Integrity Manifest Specification, version 0.15.	March 2020
	TCG Reference Integrity Manifest (RIM) Information Model, Version 1.00, Revision 0.13, 2019 TCG Reference Integrity Manifest (RIM) Information Model, Version 1.0, Revision 0.13.	December 2019
	Unified Extensible Firmware Interface Specification (UEFI), Version 2.4 (Errata B) or later.	June 2013
	TCG PC Client Platform Firmware Integrity Measurement, Version 1.0 Revision 24.	December 2019
	CSfC Continuous Monitoring Annex 1.0	August 2021
	CSfC Data At Rest Capability Package 5.0	November 2020

Document	Title	Date
	CSfC Key Management Requirements Annex 2.1	May 2022

867

868

869