Leveraging DTECH Products in a Mobile Access CSfC Solution

Abstract

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off – the - Shelf (COTS) products. The Capability Packages are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators. (https://www.nsa.gov/ia/programs/csfc_program/)

This paper provides an example of DTECH's commercial off the shelf (COTS) products being utilized to implement a CSfC Mobile Access (MA) Capability Package. The CSfC MA Capability Package describes a CSfC system that meets the demand for using commercial End User Devices (e.g. phones and tablets) to access secure enterprise services. The Mobile Access Capability Package Version 1.0 enables customers to implement layered encryption using commercial products between a Red Network infrastructure and End User Devices (EUDs).

References:

- https://www.nsa.gov/ia/_files/MA_CP_v1.1.pdf
- www.DTECHlabs.com

1 Introduction

The M3C4G Product Family consists of modular common back plane components that share a power supply, gigabit Ethernet network, and chassis.

The NSA CSfC Mobile Access Capability Package (v1.1) defines the architecture and requirements necessary to field a Mobile Access CSfC Solution. CSfC Solutions must use products from the NSA's CSfC Components list. Even though DTECH's M3C4G products don't appear directly on the CSfC Components list, DTECH M3C4G products embed CSfC components or can be used to host software that is a CSfC Approved Component.

2 Mobile Access Architecture and Components

The following Architecture diagram is sourced from the Mobile Access Capability Package document.

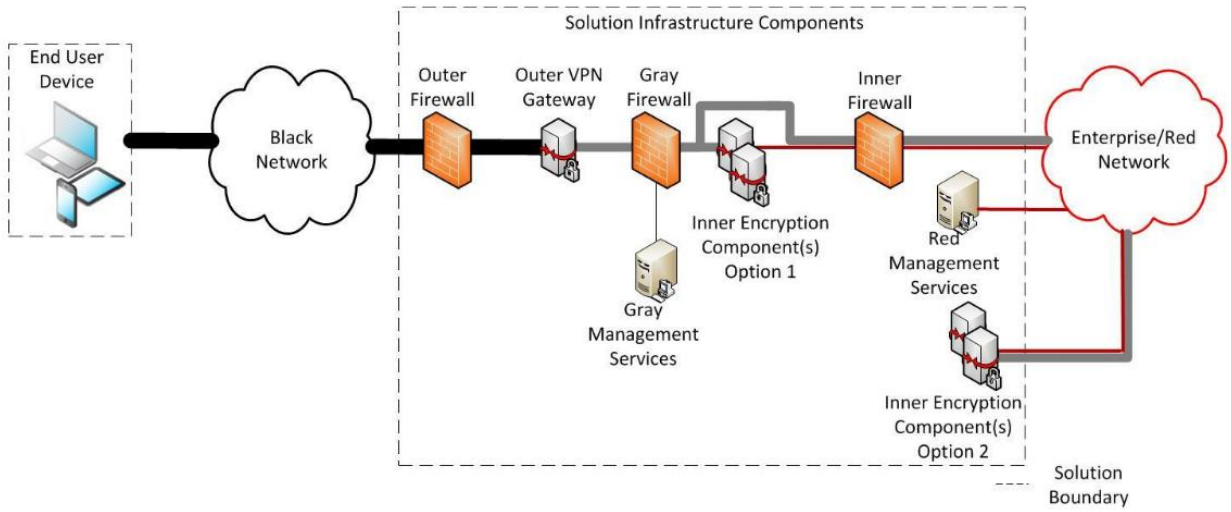

Figure 1: Two Layers of Encryption Protected Data across an Untrusted Network

2.1 End User Device Components

In the Mobile Access architecture, see Figure 1, the End User Device (EUD) is assumed to be a laptop or mobile computing platform (phone/tablet). The EUD may be 1 or 2 physical devices and it must implement 2 layers of cryptographic services to protect traffic. The 2 layers of cryptographic services may be IPsec-IPsec or IPsec-TLS. In IPsec-IPsec implementations the 2 layers must be implemented on logically diverse IP stacks.

Note that this solution only services End User Devices (EUD), and does not service remote enclaves or remote groups of devices. For remote enclave type solutions, see the VPN capability package.

2.1.1 The DTECH TXC4 as a CSfC Mobile Access EUD

DTECH products that could be utilized as components within an End User Device system include DTECH product models that are essentially computers/servers possibly combined with a router and/or network access module. A network access module, or retransmission devices as they are referred to in the capability package, provide access to the Black Network (see Figure 1).

For the purposes of this exercise the DTECH TXC4 product, shown below with an optional MANET radio module, will serve as the EUD. The use case for this TXC4 EUD is as a ruggedized vehicle mounted workstation that can be used to access classified systems. Note that such a system would require a thin client configuration (no non-volatile storage) or a Data At Rest (DAR) encryption system to fulfill this role, but this detail is not explored further in this paper.

Figure 2: TXC4 with TXC-MANET Module

The TXC4 has an embedded (CSfC approved) Cisco ESR5915 router, computer/server, and a Cisco ESS2020 switch. The internal switch interconnects the router and computer as well as the expansion module, if present.

The TXC4 in this EUD role uses the MANET radio as the black network link, the ESR5915 router as the outer VPN tunnel, and the computer/server with a VPN client, such as the Aruba VIA VPN Client, native Windows 8 IPsec stack, or Cisco AnyConnect Desktop Client, as the inner VPN. The internal computer also provides the end user terminal and user interface applications. This combination of products is 100% sourced from the CSfC Components list and is currently available for purchase and inclusion in CSfC solutions.

2.2 Mobile Access Solution Infrastructure Components

In the Mobile Access architecture, see Figure 1, the infrastructure components are assumed to be traditional data center or server room assets. However, if there is the need for providing such services in a more austere environment there is no better suited solution than a stack of DTECH M3C4G or M3-SE kit. This section defines an example of the mobile access infrastructure components using M3C4G components.

2.2.1 Mobile Access Infrastructure Overview

The Mobile Access Capability Package calls out several components, including firewalls, VPN concentrators/gateways, Certificate Authorities (CA), Intrusion Detection and Prevention Systems (IPS/IDS), workstations, and Security Information and Event Management (SIEM) assets. Each of these components has a set of requirements that limits how the component is used within the solution.

The requirements within the capability package specify that certain components must have physical isolation from other components. Specifically, the inner VPN and outer VPN components cannot share a physical embodiment with their neighboring firewall elements. This limits the minimum number of components that can fulfill the roles prescribed by the Capability Package. However, other components are permitted, or at least not explicitly disallowed, from co-locating.

A possible mapping of functional capabilities to physical assets in a DTECH M3C4G based Mobile Access Capability Package infrastructure architecture is shown in Table 1. This table is just one of the many possible combinations of DTECH products and CSfC listed components that would fulfill the roles prescribed within the Mobile Access Capability Package. Rows of the table that contain multiple functions and components are envisioned to utilize virtualization to enable the colocation of those functions and components into a single server. The use of virtualization drives down the total Cost, Size, Weight, and Power (C-SWaP) of the CSfC solution.

Table 1: DTECH M3C4G CSfC Functional to Physical Mapping

Function	M3C4G Model	CSfC Component
Outer firewall	M3-PM-SVR3	Aruba VMC
Outer VPN gateway	M3-PM-RTR3C	Cisco ESR 5915
Gray firewall, gray CA, gray SIEM, grey IPS/IDS, gray admin workstation	M3-PM-SVR3Q	Aruba VMC, Windows Server 2012 R2
Inner VPN	M3-PM-SVR3	Aruba VMC
Inner firewall, red CA, red SIEM, red IPS/IDS, red admin workstation, Red content/assets	M3-PM-SVR3Q	Aruba VMC, Windows Server 2012 R2

If DTECH products are already in use by a customer or program with traditional Type-1 equipment the existing equipment can be easily converted for use in a CSfC solution. In many cases most of the required components should already be in place and reconfiguring or adding to the solution would be a smaller effort.

Figure 3: DTECH M3C4G Products in a Hard Sided Case

DTECH M3C4G products are uniquely suited to providing CSfC solutions in austere or fielded locations. The M3C4G product line is modular and easily fits within a hard side case as shown in Figure 3. Note: the modules required to fulfill the roles identified above in Table 1 are not the models shown in Figure 3 above, but the overall system size would be the same as what is depicted in the picture.

3 Conclusion

The CSfC Mobile Access Capability Package provides government users with a set of instructions and guidance on how to go about properly using commercial products to field classified services. DTECH M3C4G and TXC product lines provide an industry leading combination of small size and rugged design that meets the requirements of government users in even the most challenging of conditions. When composing CSfC solutions to meet the NSA published CSfC Capabilities Packages DTECH products can be effectively used either directly or as host platforms across the entire spectrum of CSfC components. In those cases where DTECH equipment is already fielded or in use, modifying those systems to provide a CSfC solution would require only minimal modification or reconfiguration.

4 Points of Contact:

Nick Podolak
Senior Principal Software Engineer
CUBIC | DTECH LABS
nicholas.podolak@DTECHlabs.com
http://www.DTECHlabs.com/

Or contact an account manager at sales@DTECHlabs.com . They may assist in getting any questions answered or support needed regarding DTECH products used for CSfC or any other requirements you may have.