National Security Agency
Information Assurance
Directorate

Commercial Solutions for Classified (CSfC)
Campus IEEE 802.11 Wireless Local Area Network (WLAN)
Capability Package

Version 0.9

14 December 2012

Information Assurance Directorate (IAD)
National Security Agency (NSA)

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

FOREWORD

The Campus Institute of Electrical and Electronic Engineers (IEEE) 802.11 Wireless Local Area Network (WLAN) Capability Package is a product of the National Security Agency/Information Assurance Directorate (NSA/IAD) Mobility and Commercial Solutions for Classified (CSfC) Programs. NSA/IAD is developing new ways to leverage emerging technologies to deliver more timely Information Assurance solutions for rapidly evolving United States Government (USG) customer requirements. To satisfy this new business objective, the CSfC process was established to enable commercial products used in layered solutions to protect classified National Security Systems (NSS) and the data they carry. This process satisfies USG customers' urgent requirements to communicate securely with interoperable products based on commercial standards in a solution that can be fielded in months rather than years.

A Capability Package will:

- Provide a "Design to" package, not an exact wiring diagram for proposed solutions. System integrators will be responsible for ensuring their specific implementation reflects all the requirements defined within this Capability Package.
- Provide assurance that a solution is designed, deployed, and capable of achieving a favorable accreditation decision for the protection of classified information. The risks have been determined by NSA to be acceptable for the protection of classified information using commercial components.
- Continue to evolve through feedback provided to NSA.
- By providing the necessary documentation, enable each stakeholder to recognize design concerns, usage and environment constraints, necessary components, and assumed risk.

NSA has demonstrated the ability to securely implement the Campus WLAN solution in the lab, and an operational pilot is planned to start early 2013. This document is one in a series of releases, and will be updated to reflect lessons learned from the operational pilot. The intent of the early release of these documents is to establish a partnership between USG system integrators and NSA/IAD experts to build Secure Mobility capabilities and to establish a dialogue with industry to develop the commercially available products for those capabilities. At this time, guidance in this document may not be applied without consulting NSA's CSfC for support prior to presenting a solution to the implementing organization's Authorizing Official (AO). USG entities interested in presenting solutions to their AOs in accordance with this guidance must first submit a request for Capability Package application support to the CSfC. In the future, however, customers and their solution providers will be able to use this guidance to implement solutions without such NSA/IAD involvement.

USG entities using this Capability Package to establish their own mobility capabilities need to ensure that in doing so they comply with all relevant policies on the use, storage, and management of mobile devices and infrastructure components. USG users must also comply with all existing applicable Certification and Accreditation (C&A) requirements, such as National Institute of Standards and Technology (NIST) SP 800-53. If there is a conflict between the Mobility Capability Package Requirements and the C&A requirements, the guidance in the Capability Package takes precedence. This is because the Committee on National Security Systems (CNSS) National Manager has deemed that where NSS and the protection of classified information carried on them are concerned, the particular component layering and implementation guidance in this document is required to adequately secure the composite commercial solution. While this document is intended to allow USG entities as much

flexibility as possible in implementing a mobility capability, vendor diversity for the encryption and security critical functions is essential to the security of the overall solution. Consequently, if an agency is deciding between a solution that meets more objective requirements that is composed of products from a single vendor and a solution that meets fewer objective requirements that includes products from multiple vendors, the agency must select the multi-vendor solution, as dictated by this guidance.

The National Manager is authorized to 1) approve, and has approved, this Capability Package as an information assurance technique for securing NSS and the information they carry in the mobile environment, and 2) prescribe this Capability Package guidance as the minimum standards for a commercial solutions to protect such NSS and information in the mobile environment. (CNSS Directive (CNSSD) 502, "National Directive on Security of National Security Systems," Section 8). However, users' application of this guidance does not constitute approval or accreditation of any particular solutions developed using this Capability Package. In accordance with Section 9.b of CNSSD 502, users of this Capability Package are responsible for obtaining, under their established agency accreditation and approval processes, certification and accreditation of any mobility solution processing classified information that has been developed in accordance with this Capability Package.

Failure to properly and adequately follow the guidance in this Capability Package may reduce the security of the solution and, in the case of NSS, provide insufficient protection for NSS processing classified information, which would constitute a violation of CNSSD 502. If users applying this Capability Package and developing solutions intended to process classified information need to deviate from the requirements and guidance in this document, before their solutions may be approved and accredited for use, they must obtain a waiver from their agencies' accrediting official as well as NSA. A request for a waiver must include a detailed justification for the deviation from the Capability Package guidance. Users applying this Capability Package must also address the lifecycle of the components/solution taking into consideration component changes, routine package updates, and emergency package updates.

Customers who want to use a variant of the solution detailed in this Capability Package or to use a traditional Government Off-The-Shelf (GOTS) process must contact NSA to determine ways to obtain NSA approval. Additional information about the CSfC process will be available on the CSfC web page (http://www.nsa.gov/ia/programs/CSfC_program/index.shtml).

Please provide comments concerning the improvement of this document to mobility@nsa.gov. When submitting comments, please indicate whether you are claiming any intellectual property rights in the information you are providing and, if so, indicate which particular information you claim to be intellectual property. For more information about the NSA/IAD Mobility Program, please visit: http://www.nsa.gov/ia/programs/mobility_program/index.shtml

For more information about the CSfC program or the related National Information Assurance Program (NIAP), please visit the following web sites:

http://www.nsa.gov/ia/programs/mobility_programs/index.shtml

http://www.nsa.gov/ia/programs/CSfC_program/index.shtml

http://www.niap-ccevs.org/pp

http://www.iad.gov

DISCLAIMER

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

The User of this Capability Package 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 attorneys’ 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 Capability Package is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer’s product or service.

1 ENTERPRISE MOBILITY

1.1 Goals

Enterprise Mobility provides users with anytime, anywhere access to data, services, and other users to successfully and securely achieve their mission, whether it is war fighting, intelligence, or business. This Capability Package describes the layered security approach for using commercial WLAN and endpoint devices to securely connect mobile users to the Government enterprise. *Since secure mobile access using commercial technology is a new enterprise capability and the products and technologies are still maturing, the Capability Package is incrementally evolving towards a complete enterprise solution:*

- **Evolving Capabilities:** This release of the Campus IEEE 802.11 WLAN Capability Package is focused on enabling commercial user equipment (i.e., tablet and laptop computers) access to secure enterprise services over a campus wireless network. In the future, the Campus IEEE 802.11 WLAN Capability Package will be merged with the Mobility Capability Package to cover both commercial cellular and Wireless Fidelity (WiFi) access to classified information in National Security Systems.
- **Evolving Guidance:** The initial version of the Campus IEEE 802.11 WLAN Capability Package outlines a broad-based set of architectural, functional, and configuration requirements to support commercial mobile devices access to classified information via campus WLAN on National Security Systems. Subsequent releases will add enhanced security mechanisms and testing procedures.

1.2 Enterprise Mobility Overview

Enterprise Mobility described within this Capability Package is supported by the use of wireless devices to access sensitive data and enterprise services while minimizing the risk when connecting to existing Government enterprise networks. Government-managed campus-area wireless networks provide controlled connectivity between mobile users and the broader Government enterprise.

Figure 1-1 depicts at a high level the Campus IEEE 802.11 WLAN solution within the context of the basic segments of the Enterprise Mobility architecture.

User Equipment (UE) within this document is a commercial tablet or laptop computer that supports WiFi connectivity options and hosts data applications on a general purpose operating system environment.

- Commercial mobile devices provide widely available, cost effective, up-to-date technology for communications and application functionality. Use of these consumer-oriented devices minimizes the device cost and reduces technical obsolescence compared with Government-specified and -developed devices.
- Current commercial mobile devices have not fully addressed security issues relevant to Government operations. Enterprise Mobility will use commercially available protections that currently exist, and compensate for device limitations within the overall Enterprise Mobility architecture, primarily by leveraging the secure Government enterprise. Where necessary, commercial mobile devices may need to be hardened to protect integrity and reduce risks.
- Section 3 contains more information on User Equipment.

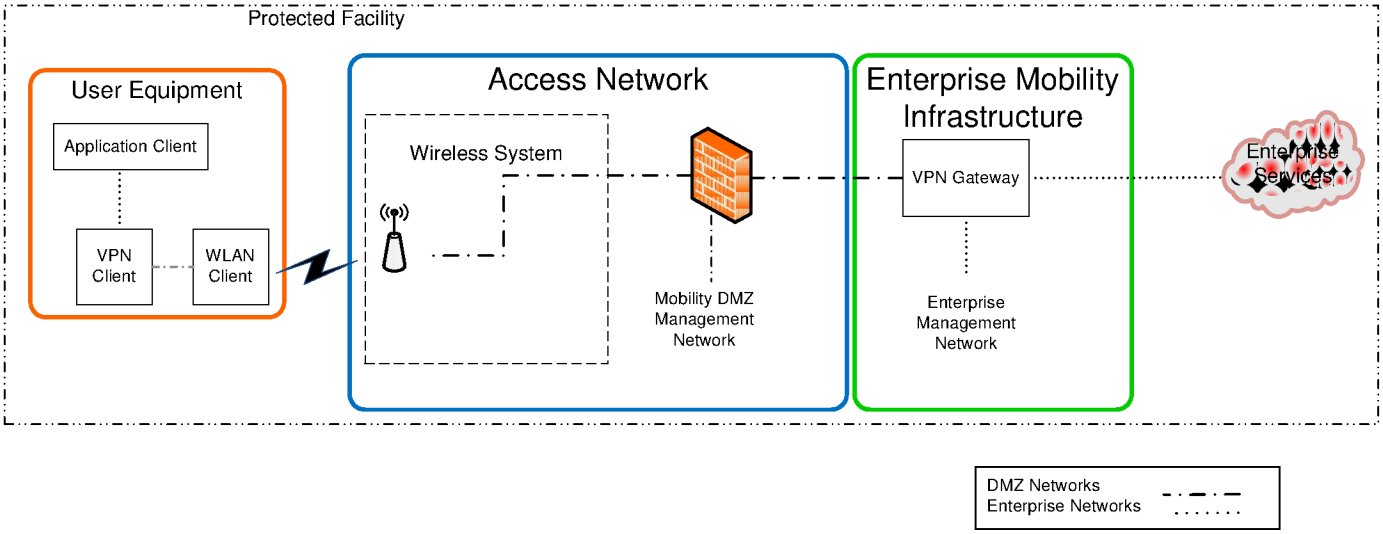

Figure 1-1. Campus IEEE 802.11 WLAN Solution within Context of Enterprise Mobility Architecture

Access Network is a Government-provided wireless access system that provides data network connectivity and capacity. These solutions can be implemented within campus area, tactical and/or deployable solutions.

Within the context of this Capability Package, an access network consists of an enterprise IEEE 802.11 WLAN supporting multiple Access Points (APs) to ensure campus-wide Radio Frequency (RF) coverage. The WLAN supports WiFi Protected Access 2 (WPA2)-Enterprise authentication based on IEEE 802.1X and relies on an external Authentication, Authorization, and Accounting (AAA) service for WLAN-wide authentication. Because traffic over the WLAN Distribution System (Access Points, switches, cabling) is only protected by a single layer of encryption, the Distribution System is considered classified at the same level as the unencrypted use data and must comply with local physical protection requirements applicable to that classification level. Section 4 contains more information on the Access Network.

Enterprise Mobility Infrastructure provides the enterprise-side termination of the secure Virtual Private Network (VPN) connection, the required administrative functions for VPN connectivity and interfaces with the Remote Access boundary of the Enterprise Services. Section 5 contains more information on the Enterprise Mobility Infrastructure.

Enterprise Services are those provided across the Remote Access boundary to mobile users by the broader Enterprise and are not an inherent part of the secure WiFi infrastructure. Most user services are hosted in the enterprise and include applications such as email, browsing, document handling, chat, presence, and (potentially) voice services.

Enterprise Services provide:

- User authentication and access controls.
- Strong boundary protection to ensure that only authorized users, devices, and permitted traffic types are allowed.
- Best practice encapsulation of business logic behind the service interface to encourage clients to be thin and lightweight; consequently, reducing the need for storing sensitive data locally.

- Enterprise monitoring of device usage and management of updates to ensure proper configuration. Section 2 contains more information on specific mobile applications and services.

1.3 Design Summary

Composed, layered solutions are the basis for the secure use of mobile devices and commercial components for access to Government enterprise services and data. Layers of commercial encryption, layers of authentication and authorization, boundary protection, possible hardening of devices, and mobile device provisioning/management all contribute to overall system security.

The following are the overarching themes for secure Enterprise Mobility capabilities:

- Employ layered Data-In-Transit protection to tunnel traffic from the mobile device to the enterprise boundary.
- Ensure that all service requests and user traffic from a mobile device are mediated through the Enterprise Mobility Infrastructure.
- Locate the bulk of security functionality and trust in the enterprise.
  - Provision and manage devices to establish and maintain secure operations.
  - Authenticate devices and users prior to authorizing network and service access.
  - Provide strong boundary protection to limit risk to Government resources.
- Wherever possible, harden commercial devices to protect integrity and reduce risks.

In order to promote interoperability and enable the use of a wide variety of commercial products, the following additional guidelines are used in the Enterprise Mobility architecture:

- Use open standards and protocols wherever possible.
- Avoid vendor lock-in, such as proprietary implementations.
- Use standards and service interfaces common with other clients (e.g., fixed, tactical) wherever practical.

In order to adequately protect sensitive information using commercial devices, the following cryptographic principles apply:

- To cross open access networks, two layers of approved commercial cryptography will be required. One of these layers will be an Internet Protocol Security (IPsec) VPN which establishes a secured path between the UE and the Enterprise Mobility Infrastructure. The other layer may depend on the particular access network and applications being used. In this Capability Package the outer layer is the WiFi Protected Access (WPA) encryption with the specified algorithm requirements. Each layer should individually have the cryptographic strength necessary for protecting the data being transported. In particular, Suite B cryptography should be used.
- Government-issued Public Key Infrastructure (PKI) credentials should be used for mutual authentication in both layers.
- The systems providing each layer of encryption must be entirely independent of each other (i.e., they cannot share application components, libraries, or hardware).

1.4 Use of the Capability Package

The main body of this Capability Package provides a narrative description of the goals of the solution and an overview of the solution, including the identification of security relevant components and their functions. The appendices address the architectural, configuration, and functional device requirements as well as operational and accreditation aspects.

- APPENDIX A: Provides architectural and configuration information that allows customers to select Commercial Off-The-Shelf (COTS) products from the CSfC Component list for their solution and to properly configure those products to achieve a level of assurance sufficient for protecting classified data.
- APPENDIX B: Provides the testing criteria for a solution implementation (to be supplied in a future release).
- APPENDIX C: Provides functional device requirements for security relevant components without a Protection Profile (otherwise, the appropriate Protection Profile provides these requirements).
- APPENDIX D: Addresses operational and accreditation aspects of usage and handling policy, role-based personnel requirements, information to support the Approving Official, and a description of securely connecting a mobile device.

2 MOBILE APPLICATIONS AND SERVICES FOR CAMPUS WLAN

2.1 Description of the Campus IEEE 802.11 WLAN Solution

The Campus IEEE 802.11 WLAN CSfC solution addresses the need to protect classified information as it travels over-the-air between a WLAN-enabled UE and a WLAN Infrastructure attached to a wired network of the same classification level. The solution also addresses the risks introduced to the enterprise network by providing a wireless interface. For this document, a campus solution is defined as a trusted Enterprise WLAN deployed in the same protected facility as the classified network it will be accessing. The UE shall be physically and administratively protected at the classification level of the enterprise network it is accessing.

As seen in Figure 2-1, the architecture enlists two layers of cryptography, one WPA2 and one IPsec VPN. Each layer should meet the requirements of CNSS Policy (CNSSP) No. 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems," dated 29 March 2010.

2.2 WLAN Architecture Components

The Campus WLAN CSfC solution consists of the following key components:

- WLAN Client (part of Mobile Device solution)
- VPN Client (part of Mobile Device solution)
- Wireless System
- Firewall Enclave
- IPsec VPN Gateway
- WLAN Authentication Server
- Wireless Intrusion Detection System (WIDS)
- Certificate Authorities
- Administration Devices
- Provisioning Systems.

2.3 WLAN Architecture Networks

There are network segments within the architecture in which the data is unencrypted, protected with only one layer of data-in-transit encryption, and protected with two layers of data-in-transit encryption. For clarity, these network segments are described by their logical location and the level of protection they provide. The following terms are used throughout this document:

- **Enterprise Network**—The network behind the IPsec VPN Gateway where the data is unencrypted. The Enterprise Network also contains the management functions for the VPN Gateway, including the VPN Certificate Authority (CA), and the administration/audit server functions.

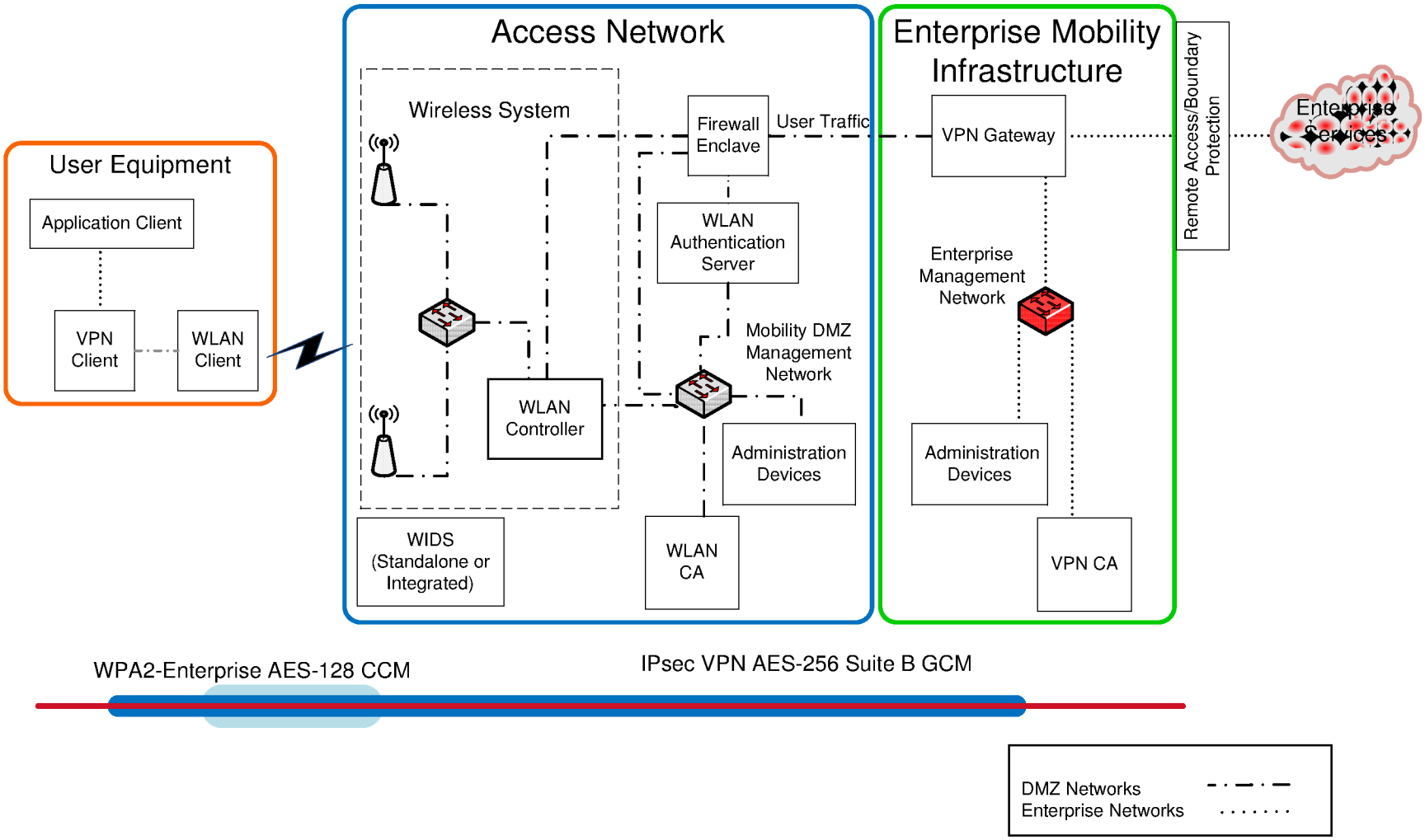

Figure 2-1. Campus WLAN Infrastructure tor Classified

- **Mobility Demilitarized Zone (DMZ) Network**—The network between the Wireless Access Points and the IPsec VPN Gateway where user data is protected by only a single layer of encryption. Devices and cables that comprise the DMZ network are treated and protected as being classified to the same level as the unencrypted user data. This network is broken down into two sub-networks:
  - DMZ Management Network—the part of the Mobility DMZ network containing the management functions to run the WLAN layer, including the Wireless System CA, WLAN Authentication Server, and the Wireless System admin/audit server functions.
  - DMZ Data Network—the part of the Mobility DMZ Network that sends data between the Wireless System and the VPN Gateway. The Mobility DMZ Data network is isolated from the Mobility DMZ Management network using either physical or virtual Local Area Networks (LANs).
- **Wireless Network**—The connection between the Mobile Device and the Wireless System in which data is protected with two layers of encryption (the VPN and the WLAN layers).

2.4 Interactions with Enterprise Services

The two layers of encryption (WLAN and VPN) required by this Capability Package result in the creation of nested secure tunnels that carry Internet Protocol (IP) packets between the mobile device and the Enterprise Mobility Infrastructure. The VPN Gateway acts as the endpoint of the inner tunnel on the infrastructure side. Integration with the back-end enterprise network on the unencrypted side of the inner tunnel is outside the scope of this Capability Package, but this section identifies some best practices. Appropriate organizational policies and directives should be consulted for definitive information.

Boundary Protection: Analogous to the guidance for remote access to unclassified networks, each packet emerging from the tunnel should be analyzed to the same degree as an un-tunneled packet arriving from an external network. The boundary protections at the tunnel exit point should include an Intrusion Detection or Prevention System (IDS or IPS) to detect network attacks followed by one or more filters to limit access to enterprise resources. The minimum suggested configuration is an IDS/IPS together with a stateful packet-filtering firewall. To provide more protection, application-level filtering may be added to verify that application protocols are well-formed and do not contain embedded malicious code.

Authentication and Authorization: The WLAN and VPN Gateway only authenticate mobile device identity using machine certificates. It is recommended (and may be required) that the mobile device user be authenticated prior to granting access to back-end application services. This verification should be centralized and occur as close to the network edge as possible.

Guidance: The following references provide useful guidance for securing remote access to enterprise resources for the Department of Defense (DoD). This guidance for securing remote access should be applied within the context of the classified network for which a wireless connection is provided.

- Secure Remote Computing (SRC) Security Technical Implementation Guide (STIG), Defense Information Systems Agency (DISA)
- Network Infrastructure Technology Overview, DISA
- Remote Access Policy STIG, DISA

- Remote Access Server (RAS) STIG, DISA

2.5 Enterprise Services

The Campus WLAN solution described in this Capability Package is application-agnostic in that it provides an end-to-end path for IP packets between the UE and the Enterprise Network without regard to what those IP packets contain. Enterprise services may or may not depend on the ability of the UE to provide local non-volatile storage for user data, configuration data, or state information (e.g., persistent cookies).

The user authentication services described in Section 2.4 may be implemented within application gateways and proxies that provide boundary protection services between the VPN Gateway and back-end enterprise application services. These boundary protection services may include application protocol validation and malicious code detection, and may forward the authenticated user identity to the application services.

3 USER EQUIPMENT

The UE, a commercial tablet or laptop computer that supports WiFi connectivity options, may run applications that make use of local processing or local persistent storage ("thick client") or "thin client" applications such as remote desktop clients. When running a "thin client" application, user data may be written to non-volatile memory (for example, to a page file). As a result, the overall UE cannot be considered a thin client device and must be protected at all times in accordance with policy applicable to the classification level of the user data it processes. This requirement remains even if Data-At-Rest (DAR) encryption capabilities are enabled, as none have been approved for protection of classified data on commercial UEs.

Figure 3-1 shows the software architecture of a typical UE. The Internet Key Exchange (IKE) application and WPA2 daemon run as operating system processes and exist to perform authentication and key establishment for the IPsec module and WLAN driver respectively. Each application should use a different user-mode cryptographic library to meet CSfC diversity requirements. As depicted, the IKE application is using its own cryptographic library, whereas the WPA2 application is using a user-mode cryptographic library supplied as part of the operating system. Encryption of the user data is often performed directly in the kernel for performance reasons. If the IPsec module and WLAN driver both use the operating system's built-in kernel-mode cryptographic library (as shown), this results in loss of cryptographic diversity even when different user-mode libraries are used for authentication and key establishment. Candidate products should be carefully evaluated to ensure the cryptographic independence of the WLAN and VPN Clients as required by CSfC.

3.1 Device Protection

The UE is the mobile device and the complex combination of functions, components, operating systems, and applications that provide a variety of security services.

The operating system of the UE is responsible for providing the following security functions to enable secure connections to the Enterprise Mobility Infrastructure and to ensure that the device operates under known, authorized conditions:

- UE protection capabilities, including:
  - System configuration—initial provisioning to remove or disable non-essential services and install required software.
  - Device monitoring—notification and logging of security faults with cessation of operations for critical events.
  - Local authentication—separate layers of authentication to provide access to the device and to the enterprise.
  - Updates— initially all updates must be provisioned through non-Over-The-Air (OTA) interaction with the UE; in the future, authenticated and authorized OTA updates will be supported.
- Local key and certificate management for the VPN and WLAN clients and other applications.
- VPN and WLAN clients—one of these may be completely implemented by the operating system or responsibility may be shared with third-party components that perform authentication and key establishment functions.

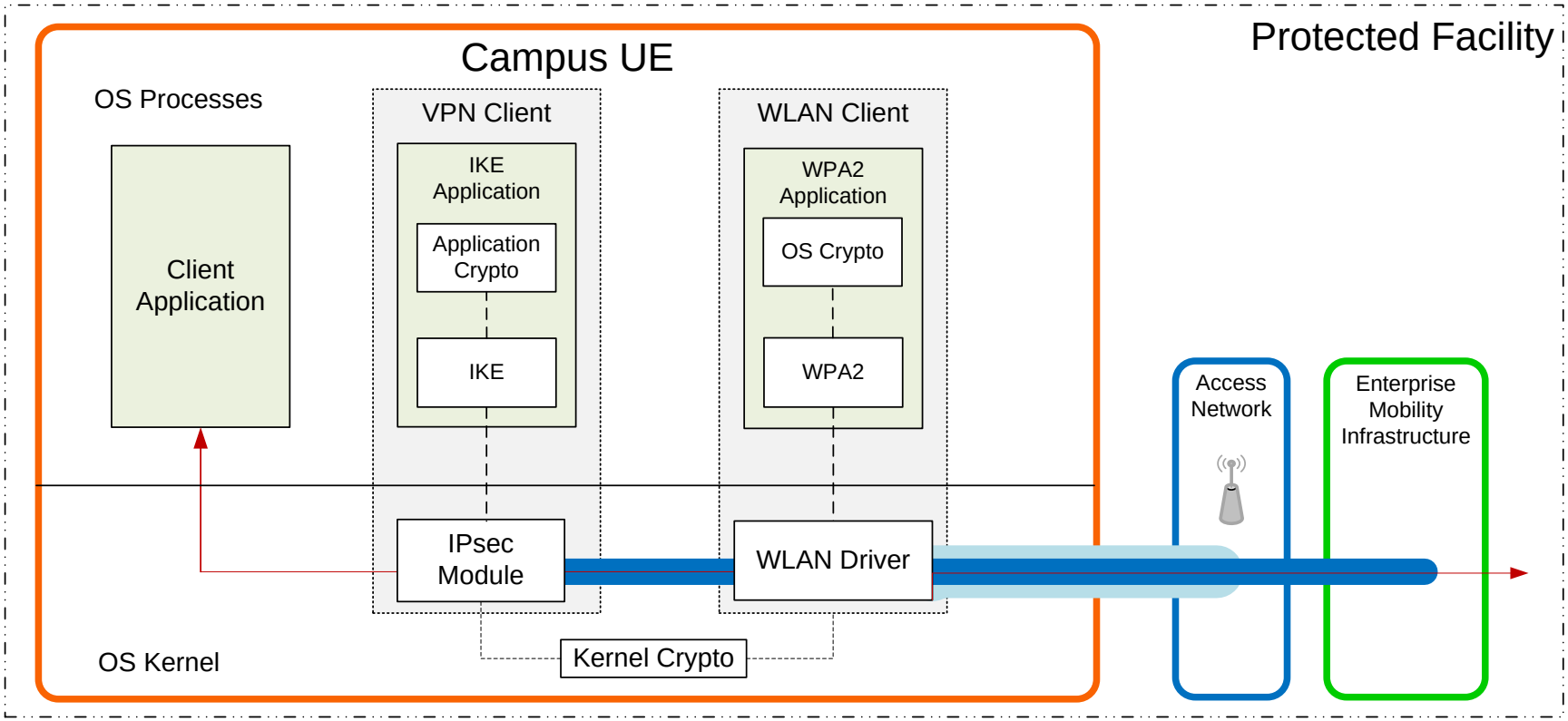

Figure 3-1. Notional Campus WLAN Mobile Device Software Architecture

3.2 WLAN Client

The WLAN Client is a software application that provides management and control of the IEEE 802.11 wireless connection. The products chosen to implement the WLAN Client services shall provide a base level of protection and shall be able to interoperate with products from other vendors. The WLAN Client automatically establishes the IEEE 802.11 WPA2 tunnel between the Mobile Device and the Wireless System using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) over IEEE 802.1X to pass Public Key machine certificates for mutual authentication between the WLAN Client and WLAN Authentication Server.

3.3 VPN Client

The VPN Client is a software application running on the Mobile Device. The products chosen to implement the VPN services shall provide cryptographic and functional services that meet or exceed the requirements listed in APPENDIX A for the VPN Client, and they should ideally also support interoperability with products from other vendors.

The VPN Client establishes an IPsec tunnel to the VPN Gateway. The VPN Client first performs an IKE exchange with the VPN Gateway to authenticate both parties and exchange session keys for the IPsec tunnel. Authentication is performed via mutual authentication of Public Key machine certificates. When IKE completes, the IPsec tunnel is secured using the Encapsulating Security Payload (ESP).

3.4 Client Applications

Client applications interact with application services located on the Enterprise network to provide functionality to end users. Client applications may be “thin” or “thick” in terms of whether they store data in local non-persistent storage.

3.5 Gap Analysis

- Currently, the UE cryptographic libraries and randomizers utilize the same processor. The vendor diversity and process separation available in today’s UEs and required by this Capability Package has been determined to provide adequate independence for current solutions. Two layers are considered independent when:
  - The implementations of each layer are from different vendors and are not derived from a common codebase.
  - The implementations of each layer do not share cryptographic functions (i.e., a shared cryptographic library or source of randomness).
  - The operation of one layer does not influence the operation of the other layer except as defined by the interface between them (i.e., covert channels are eliminated).
- Tablets may have limited management capabilities in comparison to laptops:
  - Non-essential services cannot be removed or permanently disabled.
  - Sufficient device monitoring is not currently available for tablets. Firstly, some devices do not support local access to audit logs. In addition, remote monitoring services could be provided by Mobile Device Management (MDM) software in the future. Unfortunately, some devices currently require Internet access in order to implement an MDM solution, preventing MDM use with the Campus IEEE 802.11 WLAN solution. Furthermore, most of

those that do not require Internet access do not have sufficient kernel-level Application Program Interfaces (APIs) available for the monitoring service. A forthcoming Mobility Capability Package will describe an MDM solution.

  - Updates to the tablet software cannot be performed over-the-air and in some cases cannot be performed at all without Internet access. Due to device classification, tablets may not be connected to the Internet in order to perform updates.
  - User and administrator actions on the device cannot be distinguished.
  - Administrators have limited capabilities for locking settings and preventing users from changing settings. This limitation is particularly damaging with regard to user access to wireless network settings.
  - Unwanted root certificates (preloaded) from the device cannot be removed.

- Many implementations are not able to use machine certificates issued by different Certificate Authorities for the WLAN client and VPN client without separate certificate stores. Virtualization may be functionally necessary to create these two stores and is sufficient for providing independence and separation of the two layers. However, virtual machines are not, from a security perspective, necessary to provide independence of the two layers.
- Few tablet operating systems sufficiently protect the private keys in the native certificate store. Furthermore, most do not support Elliptic Curve Digital Signature Algorithm (ECDSA) certificates in the native certificate store. Thus, Suite B capable WLAN and VPN clients have an application-layer certificate store. These application stores often do not provide basic protections such as encrypting the private keys or preventing manipulation by other applications. Both native and application certificate stores should be implemented with key generation inside an approved Federal Information Processing Standard (FIPS) 140-2 level 2 or higher module and with an API, such as one meeting Public Key Cryptography Standard (PKCS) #11, that prevents the private key from leaving the cryptographic boundary of the store. To enable use of the devices outside a secure facility, future requirements may include token-based certificates or password protection of the private keys stored on the device.
- The WiFi Alliance is an industry standards body that certifies WiFi-enabled products against the IEEE 802.11 and TLS standards to ensure interoperability of vendor products. The Alliance's WPA2 certification requires an EAP method for authentication, for which TLS 1.0 is suggested as a minimum. TLS 1.0 allows Elliptic Curve Cryptography but does not support the Secure Hash Algorithm 2 (SHA-2) family which is what is required to meet the Suite B objectives of this Capability Package. The WiFi alliance does not currently recommend or test for TLS 1.2. The WiFi Alliance needs to be urged to test for TLS 1.2 as an option in order to influence the vendors to also adopt TLS 1.2.
- There is limited DAR protection for non-thin client deployments of tablets. Full Disk Encryption (FDE) products are available for laptops and some tablets. Current commercial DAR products are not approved to protect classified information, so the device must be handled as classified even when encrypted and powered off.
- A trusted boot capability based on a hardware root-of-trust to interact with a Network Access Controller (NAC) in the Enterprise Mobility Infrastructure is needed to attest to the hardware and software integrity of the UE. Not all UEs support trusted boot capabilities, and any trusted

boot capabilities currently developed may not allow interaction with a network controller within the enterprise.

- Not all UEs support the required security capabilities to directly connect to enterprise networks via wired connections such as docking stations. For instance, they may not support the various host-based security services generally required for devices connecting to classified networks. Even for laptops that can host the required security services, no currently approved configuration supports both wired and WLAN connectivity. Thus, users are not permitted to connect Campus WLAN UEs to the enterprise network via wired connections or to connect the device to a computer with a wired connection to the enterprise network.

4 ACCESS NETWORKS

4.1 IEEE 802.11 Campus WLAN

4.1.1 Wireless System

In the context of this solution, the APs, WLAN Controller, and the switch compose the “Wireless System.” These components are grouped together in this document to maintain vendor neutrality; there are a variety of wireless system implementations across the vendor community.

An AP is the media converter providing a link between the WLAN Client and the wired switch. The level of functionality contained within the APs is vendor-dependent. Some solutions utilize “smart” or “thick” APs which incorporate a significant amount of functionality, including cryptographic operations, whereas other solutions implement “thin” APs that merely perform the wireless/wired media conversion and push all functionality to the WLAN Controller. Some vendors may produce both types of solution. These differences impact physical protection requirements as traffic over the WLAN Distribution System may only be protected by a single layer of encryption and therefore be considered classified.

The Wireless System shall be capable of initiating and terminating multiple IEEE 802.11 cryptographic tunnels to and from numerous Wireless Clients. It shall also be capable of translating EAP-TLS over IEEE

802.1X messages to EAP-TLS over Remote Authentication Dial In User Service (RADIUS) messages to pass authentication information between the WLAN Client and WLAN Authentication Server. As part of this exchange, a pre-master key (PMK) is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes the PMK to the Wireless System over an encrypted session. The Wireless Controller and the WLAN Client use the PMK to negotiate a session key to protect the subsequent user traffic exchanged between the WLAN Client and the Wireless System. The Wireless System should operate on its own separate hardware and/or virtual device(s); depending on the vendor implementation, as mentioned above, this separation may include isolating the switches and wiring between the APs and the controller from any existing network. At the very least, the Wireless System and the VPN Gateway shall operate on separate hardware or virtual machines

4.1.2 Wireless Intrusion Detection System

An IEEE 802.11 WIDS consists of a group of sensors (preferably some dedicated) and a central controller working together to provide 24/7 monitoring of the wireless spectrum to detect unauthorized WLAN activity. The system can either be stand-alone or integrated into the WLAN controller. For the stand-alone case, ideally, information between the sensors and the controller will pass over a separate network dedicated to the WIDS, but an acceptable option is to connect the sensors over a virtual LAN established over the same wired network as used by the Wireless APs. For an integrated WIDS, whether the sensors can be placed on the Wireless network or must be placed on the Mobility DMZ network depends on the vendor’s implementation.

4.1.3 Firewall Enclave

The Firewall Enclave is located between the Wireless System and the VPN Gateway and serves multiple purposes. The Firewall Enclave protects the VPN Gateway and all the Mobility DMZ network components. The Firewall Enclave consists of two devices, a screening router and a traditional firewall appliance, that work in tandem to isolate the VPN Gateway from the Wireless System. The Firewall Enclave performs deep packet inspection to only allow valid IKE/IPsec traffic sent from the Wireless

System to enter the WLAN Authentication Server domain and the VPN Gateway domain. The Firewall Enclave also ensures that the VPN Gateway and the WLAN Authentication Server cannot initiate a connection to the Wireless System. The firewall appliance may be the same as the VPN gateway. The screening router should be physically separate from the firewall appliance but may be shared with some other component (e.g., switch, controller, router).

4.1.4 WLAN Authentication Server

WLAN Authentication Server performs device authentication during the IEEE 802.1X exchange. The Wireless Client and WLAN Authentication Server perform an EAP-TLS exchange using the IEEE 802.1X protocol, with the wireless system acting as a pass-through. As part of this exchange, a shared session key is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes this key to the Wireless System over an encrypted session to protect the subsequent user traffic exchanged between the WLAN Client and the Wireless System. The WLAN Authentication Server should operate on a separate hardware device from the Wireless System.

4.1.5 Administration Devices

The WLAN and VPN devices shall each have administration machines on the Mobility DMZ Management network that allows for maintaining, monitoring, and controlling all security functionality for the particular device. These administration devices shall also allow for logging and configuration management, as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the WLAN and VPN devices. The administration devices for the VPN are located on the Enterprise management network and the administration devices for the WLAN are located on the Mobility DMZ management network. Layer 3 routing between management and operational networks should be prohibited to maintain strict separation between management and operational traffic.

A Network-based Intrusion Detection System (NIDS) is deployed on the Mobility DMZ network. The NIDS must be regularly updated with attack signatures. It is recommended that a separate NIDS also be deployed on the Enterprise network to monitor tunneled IP traffic being decrypted by the VPN Gateway.

Infrastructure components (servers and workstations) should be configured with Host-based IDS (HIDS) software in accordance with agency policy.

4.1.6 Certificate Authority (PKI and Key Management)

No single CA can provide keys to both the WLAN devices (Wireless System and WLAN Client) and VPN devices (VPN Gateway and VPN Client). The WLAN and VPN are each supported by its own CA.

Two separate CA services are used to support the two layers of data-in-transit encryption (WLAN and VPN) in this Capability Package. Each CA service provides independent key services to the WLAN and VPN clients respectively, and the corresponding infrastructure components:

- User Equipment registration services.
- Certificate issuance services.
- Certificate renewal services.
- Certificate Revocation Services (via Certificate Revocation Lists (CRLs) and/or Online Certificate Status Protocol (OCSP).

Deploying two CA services decreases the risk to the infrastructure as they provide two independent points of failure. In addition, because they provide a signer for key pairs these Certificate Authorities provide the third party trust between the users of certificates. Both the User Equipment clients and the infrastructure components are issued certificates. Each has a critical role to play in verifying the trust of the other party as they connect in the wireless environment. The WLAN Authentication Server checks certificate revocation status prior to allowing a device to connect to the Mobility DMZ. Similarly, the VPN Gateway checks certificate revocation status prior to allowing a device to connect to the Enterprise network.

As part of an overall PKI solution, certificate revocation information should be made available to, and checked by, infrastructure components. Any compromised UE must be removed from WLAN database and VPN database. The UE's certificates are revoked at the WLAN CA and VPN CA, and new CRLs are issued. The user equipment is disconnected from the WLAN and the VPN in order to force a re-authentication. Thus, in the absence of a certificate revocation capability, a compromised UE will be explicitly de-authorized at the WLAN Authentication Server and VPN Gateway. As private keys on infrastructure components are comparatively secure, the cost of making certificate revocation information available to UEs may outweigh the benefit of doing so.

Each PKI used in the solution shall have an approved security policy that addresses certificate generation, handling, distribution, storage, destruction, and key recovery and compromise recovery. Refer to NIST SP 800-57 for guidance.

The CA for the WLAN devices shall be located in the Mobility DMZ management network. Since the Mobility DMZ management network is a small local network, a locally managed CA will usually need to be developed to support the WLAN devices, requiring that a CA product be selected from the CSfC component list for the WLAN PKI.

Each CA should operate on a single-function machine, but the CAs may be operated as virtual machines (i.e., the WLAN Authentication server and the WLAN CA may be Virtual Machines (VMs) on the same hardware platform).

4.2 Gap Analysis

- WLAN encryption is limited to 128-bit Advanced Encryption Standard (AES-128) Counter with Cipher Block Chaining Message Authentication Code (CCM) mode because the IEEE 802.11 Specification does not support any other cipher modes. Support for AES-256 and Galois Counter Mode (GCM) has been proposed for IEEE 802.11ac and is expected to become a requirement in a later version of this Capability Package.
- As with the WLAN clients, WLAN Authentication servers do not support TLS 1.2 for EAP-TLS.
- Most WIDS currently do provide enough flexibility in creating custom intrusion event signatures. The most flexible way to do this would be to allow the administrator to combine filters on every field in any IEEE 802.11 frame, including those encapsulating EAP-TLS, using Boolean logic.
- WIDS do not perform advanced statistical analysis of the monitored network. The system should take advantage of modern machine learning techniques to perform statistical analysis of the wireless traffic of individual devices and of the monitored network as a whole.
- During initial keying, the certificate from the WLAN CA is obtained first, and then the certificate from the VPN CA is obtained so that the process proceeds from Mobility DMZ network to Enterprise

network. Current certificate renewal processes would require the device to be connected to the Mobility DMZ network after it has connected to the Enterprise network. This process has undetermined risk and is not authorized as a part of this solution. As a result, this Capability Package allows for longer certificate validity periods than DOD Instruction 8420.01 recommends. With the longer validity period, it is expected either that the UE will be replaced before the time of certificate expiration or that this Capability Package will be revised to include rekeying procedures.

5 ENTERPRISE MOBILITY INFRASTRUCTURE

5.1 Objective Enterprise Mobility Infrastructure Architecture

The Enterprise Mobility Infrastructure acts as the interface between the Access Network and Enterprise Services.

In the Campus WLAN architecture, the Enterprise Mobility Infrastructure includes the VPN Gateway, the Enterprise management network associated with the VPN Gateway, and Provisioning Systems. This includes the VPN CA if this CA is dedicated to issuing certificates to the VPN Gateway and its peers.

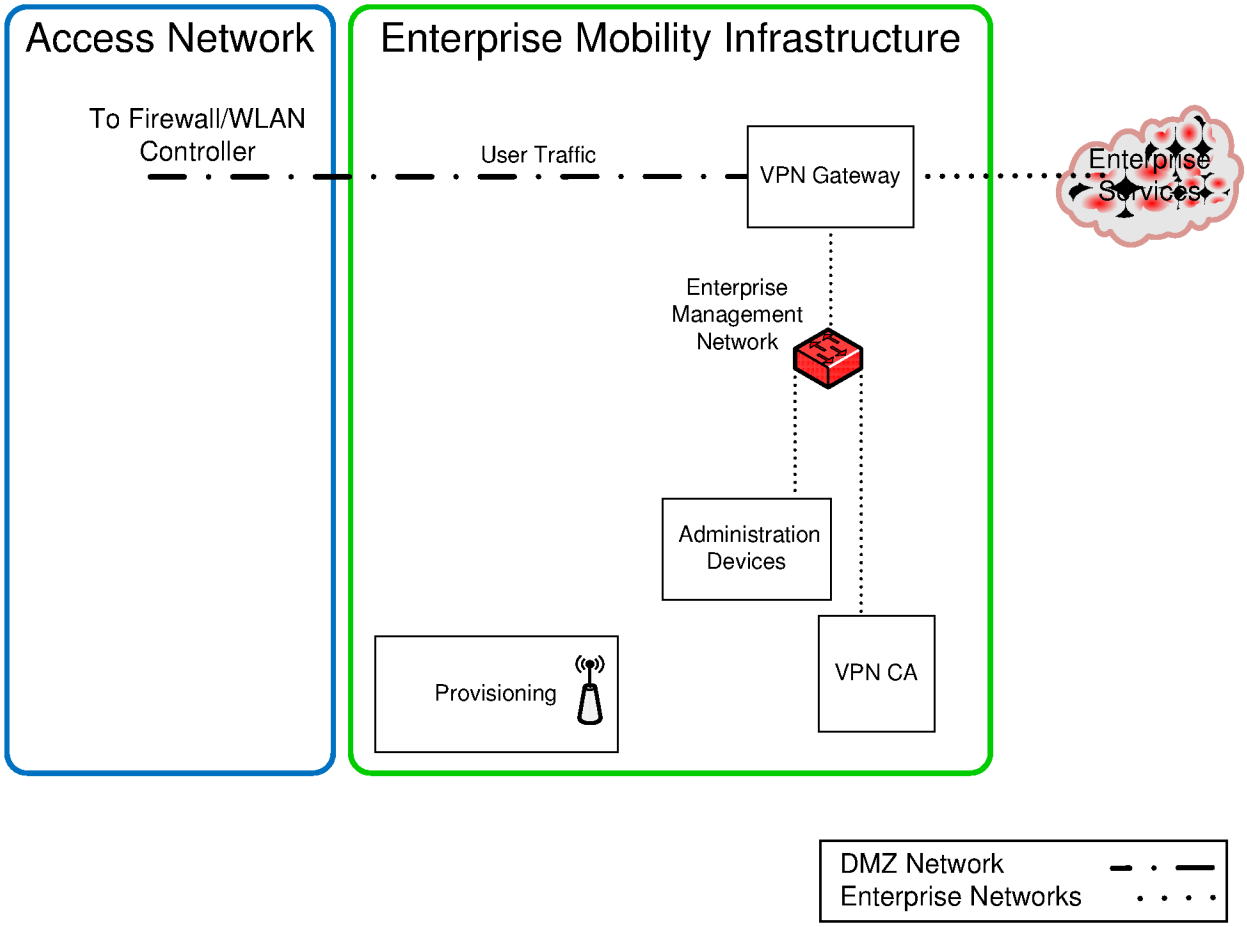

Figure 5-1. Enterprise Mobility Infrastructure for Campus WLAN

5.2 Security Relevant Components

5.2.1 VPN Gateway

The VPN Gateway is an integral part of the security of the Campus IEEE 802.11 WLAN solution and is located on the edge of the secure wired network. It serves as the endpoint of the IPsec VPN tunnel from the Mobile Device and performs a number of cryptographic functions related to establishing and maintaining these tunnels. The VPN Gateway is responsible for authenticating the machine certificate of the Mobile Device, including checking for certificate revocation information during the IPsec VPN tunnel establishment. The VPN Gateway should operate on its own separate hardware device.

5.2.2 Administration Devices

The WLAN and VPN devices shall each have administration machines on a management LAN or Virtual LAN (VLAN) separate from the enterprise data LAN or VLAN that allows for maintaining, monitoring, and controlling all security functionality for the particular device. These administration devices shall also allow for logging and configuration management, as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the WLAN and VPN devices. The administration devices for the VPN are located on the Enterprise management network and the administration devices for the WLAN are located on the Mobility DMZ management network. Layer 3 routing between management and operational networks should be prohibited to maintain strict separation between management and operational traffic.

5.2.3 Certificate Authority

The CA for the VPN devices shall be located on the Enterprise network, which allows for use of existing enterprise CAs already operational on the Enterprise network. For example, a solution may utilize an enterprise CA (such as a CNSS-approved CA, which follows CNSS Instruction (CNSSI) 1300 under the NSS PKI Root CA) to key the VPN devices. The VPN CA must issue only device certificates and may not issue user certificates.

Implementations not able to take advantage of existing PKIs for the IPsec tunnel will need to deploy a locally managed CA to support VPN devices. For each local CA, a Certificate Policy (CP)/Certification Practice Statement (CPS) document shall be developed and tailored to the specific network environment. It is the responsibility of the Approving Official (AO) to approve the use of these CAs. Refer to Section 4.1.6 for further description of CA services.

5.2.4 Provisioning Systems

Initial provisioning of campus mobile devices will be performed using enrollment capabilities hosted in the Enterprise Mobility Infrastructure and leveraging the WLAN and VPN CAs. To support different device types, it may be necessary to support both a wireless and wired connection capability to the mobile device being provisioned. Since keying and secure applications needed to connect to the operational wireless system have not yet been established, wireless provisioning connectivity must be performed on a separate wireless system in a shielded enclosure. The provisioning process includes assigning identifiers to the devices, installing required applications, configuring the device's policy and settings (especially WLAN and VPN settings), and loading certificates and keying material. Prior to provisioning devices, configuration profiles are created and required device applications are obtained.

Initial provisioning (for all device types) should include—note that a specific sequence is not implied:

1. **Device registration**. Collect identifying information from the mobile device, assign Government device identities for the Mobility DMZ and Enterprise domains, and update data stores (directory, inventory, and/or authorization) to include new mobile device.
2. **Profile and settings configuration**. Load configuration profiles (within the limitations of what is supported by each device type) that implement policies on allowed and disallowed services (such as Bluetooth) and user authentication parameters (such as password length and when to lock the device). Supply other settings such as network parameters.
3. **Application installation**. Load required applications including the VPN client and enterprise client applications (there is no current support for an online application store so all applications

should be loaded during initial provisioning). If possible unneeded applications should be removed from the device.

4. **Certificate request and issuance**. Using the assigned Government device identifiers, connect to the Mobility DMZ network, request certificates from the WLAN CA, and load received material into the mobile device. Disconnect the device from Mobility DMZ network, connect to the Enterprise network, request certificates from the VPN CA, and load received material into the mobile device.

Depending on the capabilities of the device, the device is connected and interacts with the CAs in order to be issued certificates, or the certificates are generated and loaded onto a device storage medium from a Provisioning workstation for transfer to the mobile device. There will also be differences based on whether the mobile device generates and provides a private key for the certificate or is issued one from the CA (more secure handling and transfer is required for the latter case). Finally, some devices may require that certificate provisioning be performed using a wireless connection. In the event that a device can only support wireless certificate provisioning, the certificate provisioning must be performed in a shielded enclosure. Figure 5-2 shows a possible configuration of Provisioning systems including a shielded enclosure with isolated wireless connectivity.

Once the mobile device is properly configured and certificates/keying material is in place, it is ready to be issued to a user with the final steps of establishing user login and associating the user with the device in the registration data.

If the implementing organization already has provisioning capabilities for classified UEs, then they will need to be modified and augmented to support device registration with the Mobility DMZ and certificate issuance from the WLAN and VPN CAs. If this is the first use of classified UEs within the implementing organization, then this section provides an overview of the services and systems needed to provision them.

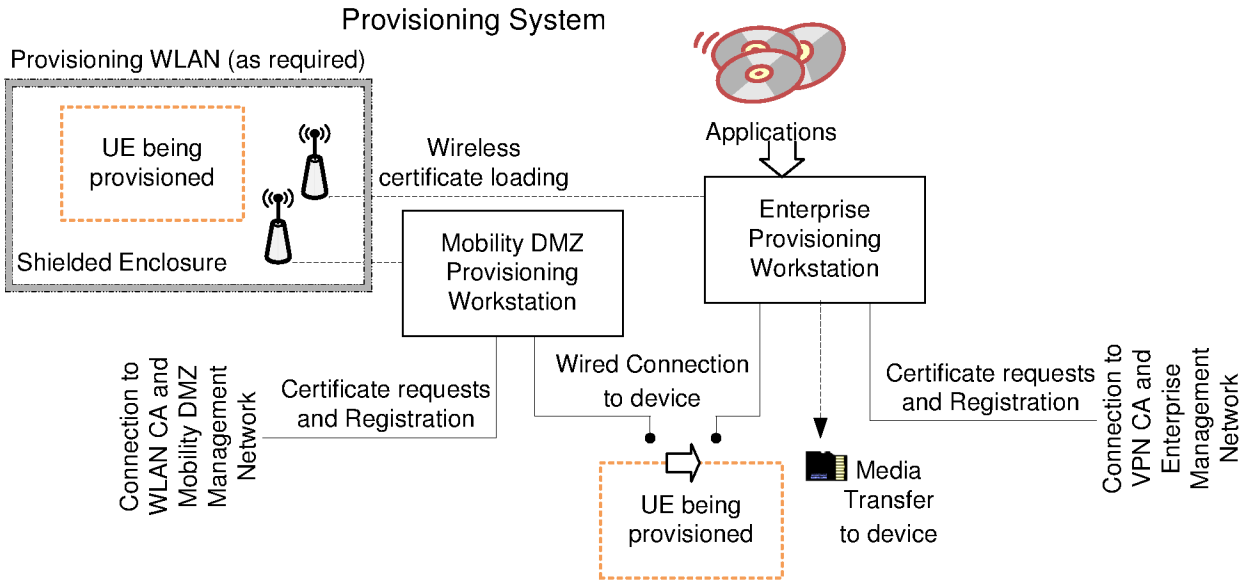

Figure 5-2. Provisioning and Key Loading for Campus WLAN

5.3 Gap Analysis

- There is a lack of inter-vendor interoperability between VPN Clients and VPN Gateways. The Campus WLAN solution currently requires the same vendor for the VPN Client as the VPN Gateway.
- The provisioning capabilities of some UEs are limited; thus, the provisioning process described above does not scale well. Furthermore, a subset of these UEs requires wireless provisioning.
- Enterprise application stores are not yet available for classified network use. Issues to be resolved before providing this capability include: required use of notification services currently only available on the Internet, enterprise process for vetting and signing of applications, and MDM capabilities to manage whitelisting/blacklisting of applications.

6 MOBILITY THREATS, RISKS, AND MITIGATIONS

The use of commercial UEs and layered commercial products to access enterprise services over a campus IEEE 802.11 wireless local area network exposes the enterprise and its data to increased risk when compared with wired solutions. The threats to the Campus WLAN use include actions taken by an adversary or an authorized user acting inappropriately. This Capability Package defines a number of ways to mitigate the risks posed to secure mobility solutions.

The full risk assessment of the Campus IEEE 802.11 WLAN solution presented in this Capability Package summarizes the types of attacks that are feasible against this solution and the mitigations that can be employed. The classified risk assessment document for the Campus WLAN solution is available on the SECRET Internet Protocol Router Network (SIPRNet) CSfC website. The AO shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

6.1 Threats

Some principal threat areas to address:

- Adversary attacks on mobile devices from rogue access points.
- Adversary exploitation of lost or stolen mobile devices:
  - Making unauthorized modifications then returning to user
  - Accessing content
  - Masquerading as authorized user
- Adversary introduction of unauthorized device modifications either remotely or within the supply chain.
- Unauthorized users and devices attempts to access the Campus WLAN.
- Authorized mobile device user misuse of privileges, such as by trying to use disallowed services/applications or trying to connect to unauthorized networks.
- Authorized operators within the Access Network and Enterprise Mobility Infrastructure misuse of privileges; particularly operators responsible for provisioning devices.
- Authorized users or operators access of multiple security domains with the mobile device.
- Adversary collection or monitoring of traffic (e.g., traffic analysis or sniffing the network) that is passing through a network or OTA.
- Adversary interference with signal or WLAN components.

6.2 Risks

Some principal risks to be prevented or mitigated include:

- Exfiltration or monitoring of sensitive data communications over the campus WLAN.
- Advanced Persistent Threat (APT) on mobile device or within Access Network or Enterprise Mobility infrastructure.
- Unauthorized modifications of mobile devices or infrastructure components creating an insecure state.
- Compromise of sensitive data being stored unprotected on mobile devices.

- Loss of authentication credential such as private keys for certificates.
- Disruption of services.
- Compromise of sensitive data through connections to rogue access points or unauthorized networks.

6.3 Risk Mitigations

There are a number of ways to mitigate the risks posed to secure mobility, and most work in concert with one another.

6.3.1 Baseline Mitigations

- **Device Hardening:** Minimum configuration requirements described within this Capability Package provide some level of device hardening. Where possible, mandatory and/or best practice hardening guidance specific to the equipment/operating system of devices within the solution should be followed.
- **System Administration Best Practices:** As with the secure operation of all systems, administrators should conduct routine audits of system logs, device firmware updates, physical inspections, etc., in accordance with best practices.
- **Layered Security:** Data in Transit protection, authentication, and authorization are implemented separately and independently for the Access Network and Enterprise Mobility Infrastructure and are supported by separate and independent PKI systems.
- **Separation of Roles:** Security critical roles will be performed by separate individuals, and the CA Administrator for the WLAN CA will be different than the CA Administrator for the VPN CA (see Section D.2 in APPENDIX D for definitions of roles).

6.3.2 User Equipment

- **User Training and Policy Enforcement:** For those threats and risk for which no technical mitigation is available or feasible, the establishment of policies restricting user behaviors and of associated user training is required.
- **User Equipment Treated as Classified:** For this campus solution, the user equipment will be treated as classified material. This restriction provides the protections associated with handling classified information and provides an assumed level of user screening.
- **Anti-Tamper Technology Deployment:** Additional protection can be provided to ensure unauthorized physical modification of the device is quickly detected through the deployment of anti-tamper technologies.
- **Separation of User Equipment Device Credentials and User Credentials:** The credentials used by the user equipment to establish connectivity across the wireless infrastructure are separate and distinct from those used to access enterprise network resources.

6.3.3 Access Network

- **Encrypted Data in Transit to Access Network:** Data transiting the wireless infrastructure to the Access Network is double-encrypted, as described in the requirements of this Capability Package, to ensure sufficient protection from eavesdropping and to limit access to both the User Equipment and Access Network endpoints.

- **Revocation Capability and Access Control:** The WLAN CA will provide timely capabilities to revoke certificates and to disseminate the certificate revocation status. The database of authorized WLAN users also provides effective management of user access.
- **Wireless Intrusion Detection System (WIDS):** WIDS placed at appropriate locations in proximity to the wireless access network usage areas provide a variety of protections for the overall solution including: detection of rogue access points, monitoring of the provisioning process, detection of known or potentially malicious traffic, and monitoring for unauthorized exfiltration of data.
- **Hardware Firewall:** Placed at key locations within the infrastructure, firewall devices ensure that components receive only the traffic which is intended and of the appropriate format for those components. Inappropriate traffic will be blocked/dropped.

6.3.4 Enterprise Mobility Infrastructure

- **Encrypted Data in Transit to Mobility DMZ Network:** Data transiting the Access Network to the Mobility DMZ is encrypted as described in the requirements of this Capability Package to ensure sufficient protection from eavesdropping and to limit access to both the User Equipment and Mobility DMZ endpoints.
- **Revocation Capability and Access Control:** The VPN CA will provide timely capabilities to revoke certificates and to disseminate the certificate revocation status. The database of authorized VPN users also provides effective management of user access.
- **Protected Enclosure:** If only wireless provisioning is supported by the mobile device, then the wireless provision of device credentials must take place within an RF protected enclosure as described within the Capability Package requirements.
- **Strong Encryption/Passwords:** Throughout the provisioning process, data exchanges take place with strongly encrypted connections and make use of strong passwords to prevent tampering.

ACRONYMS AND TERMS

Acronym List

Acronym	Definition
A/C	Architecture/Configuration
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AIS	Automated Information System
AO	Authorizing Official/Approving Official
AP	Access Point
API	Application Program Interface
APT	Advanced Persistent Threat
ASCII	American Standard Code for Information Interchange
AU	Requirements for Auditing
C&A	Certification and Accreditation
CA	Certificate Authority
CAA	Certificate Authority Administrator
CBC	Cipher Block Chaining
CCD	Configuration Change Detection
CCM	Counter with Cipher Block Chaining Message Authentication Code
CM	Cryptographic Module
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-The-Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
DA	Device Administration
DAR	Data-At-Rest
dB	Decibel
DH	Diffie-Hellman
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DN	Distinguished Name
DoD	Department of Defense
DoDI	DoD Instruction
DoS	Denial-of-Service
DPI	Deep Packet Inspection
DSS	Digital Signature Standard

Acronym	Definition
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ECP	Elliptic Curve modulo a Prime
ESP	Encapsulating Security Payload
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FW	Firewall
GCM	Galois Counter Mode
GHz	Gigahertz
GOTS	Government Off-The-Shelf
GTK	Group Temporal Key
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transport Protocol Secure
IA	Information Assurance
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alert
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange Version 2
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
KM	Key Management
LAN	Local Area Network
MAC	Medium Access Control
MDM	Mobile Device Management
NAC	Network Access Controller
NDPP	Network Device Protection Profile
NIAP	National Information Assurance Partnership
NIDS	Network-based Intrusion Detection System

Acronym	Definition
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security System
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OTA	Over-The-Air
PHY	Physical Layer
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PMK	Pair-wise Master Key
PP	Protection Profile
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Server
RF	Radio Frequency
RFC	Request for Comments
RI	Remote Interface
RSA	Rivest, Shamir, Adelman
S	SECRET
S3	Secure Sharing Suite
SA	Security Association
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIPRNet	SECRET Internet Protocol Router Network
SNMP	Simple Network Management Protocol
SP	(NIST) Special Publication
SRC	Secure Remote Computing
SSH	Secure Shell
SSID	Service Set Identifier
STIG	Security Technical Implementation Guide
TLS	Transport Layer Security
TS	TOP SECRET
UDP	User Datagram Protocol
UE	User Equipment
USG	United States Government
VC	VPN Client
VG	VPN Gateway
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

Acronym	Definition
WC	WLAN Client
WIDS	Wireless Intrusion Detection System
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wifi Protected Access
WPA2	WiFi Protected Access 2
WS	WLAN System
WUE	WLAN User Equipment

Glossary of Terms

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

Authorizing Official (AO)—A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (NIST SP 800-53)

Assurance—A measure of confidence that the security features and architecture of an Automated Information System (AIS) accurately mediate and enforce the security policy. The certification by designated technical personnel of the extent to which design and implementation of the system meets specified technical requirement for achieving adequate data security.

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 identity the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective action are required.

Availability—Assurance that the system and its associated assets are accessible and protected against denial or service attacks, as well as available when the user needs them and in the form needed by the user.

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

Capability Package—The set of guidance provided by NSA that describes recommended approaches to composing COTS devices to protect classified information for a particular class of security problem. This package will point to potential products that can be utilized as part of this solution.

Certification—The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process that establishes the extent to which a particular computer system design and implementation meets a set of specified security requirements.

Certification and Accreditation (C&A)—A comprehensive assessment of the management operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

Certificate Authority (CA)—An authority trusted by one or more users to create and assign certificates. [ISO 9594-8]

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

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

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

Edge Device—Another term for mobile device as described in this Capability Package, frequently used in Key Management requirements.

External Interface—The interface on a VPN device that connects to the outer network (i.e., the Mobility DMZ network on the VPN device or the Wireless network on the WLAN device).

Federal Information Processing Standard (FIPS)—A set of standards that describes the handling and processing of information within governmental agencies.

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

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.

Wireless Intrusion Detection System (WIDS)—A group of sensors and a central controller working together to provide 24/7 monitoring of the IEEE 802.11 wireless spectrum for intrusion attempts, denial

of service attacks, unauthorized devices attempting to connect, and authorized devices that are not following the defined security profile.

REFERENCES

The standards listed in this table may be periodically updated or superseded by their respective standards organizations. Each version of this Capability Package references the relevant standards at time of publication. If a vendor claims compliance to a more recent version of a standard than the one listed, contact NSA for guidance.

CNSS 4009	*CNSS 4009, National Information Assurance (IA) Glossary Committee for National Security Systems* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2010
CNSSI 1300	*CNSS Instruction (CNSSI) 1300, Instruction For National Security Systems Public Key Infrastructure X.509 Certificate Policy*	June 2011
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 on National Security Systems*	March 2010
DoDI 8420.01	*DoD Instruction 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*	November 2009
FIPS 140-2	*Federal Information Processing Standard (FIPS) 140-2, Security Requirements For Cryptographic Modules.* http://csrc.nist.gov/publications/fips/fips 140-2/fips1402.pdf	May 2001
FIPS 180-4	*Federal Information Processing Standard (FIPS)180-4, Secure Hash Standard (SHS).* http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf	March 2012
FIPS 186-3	*Federal Information Processing Standard (FIPS) 186-3, Digital Signature Standard (DSS).* http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf	June 2009
FIPS 197	*Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES).* http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf	November 2001
IEEE 802.1X	*IEEE 802.1X, Port-based Network Access Control*	February 2010
IEEE 802.11	*IEEE 802.11-2012, Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*	March 2012
IEEE 802.11i	*IEEE 802.11i-2004, Amendment 6: Medium Access Control (MAC) Security Enhancements*	July 2004
ITU-T X.509	*International Telecommunication Union (ITU) Recommendation X.509, Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*	November 2008
NIAP Authentication Server PP	*Authentication Server Protection Profile.* http://www.niap-ccevs.org/pp/draft_pps/	TBD
NIAP IPsec VPN Client PP	*IPsec VPN Client Protection Profile.* http://www.niap-ccevs.org/pp	January 2012
NIAP IPsec VPN Gateway PP	*IPsec VPN Gateway Extended Package.* http://www.niap-ccevs.org/pp/draft_pps/	Publication expected Q4 2012
NIAP Firewall PP	*Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall*	December 2011

NIAP WLAN Access System PP	*Protection Profile for Wireless Local Area Network (WLAN) Access System.* http://www.niap-ccevs.org/pp/draft_pps/	November 2011
NIAP WLAN Client PP	*Protection Profile for Wireless Local Area Network (WLAN) Client.* http://www.niap-ccevs.org/pp/draft_pps/	November 2011
NIAP Mobile Endpoint App PP	*Mobile Endpoint Operating System Protection Profile.* http://www.niap-ccevs.org/pp/draft_pps/	Publication expected Q4 2012
NIAP Mobile Endpoint App PP	*Mobile Endpoint Application Protection Profile.* http://www.niap-ccevs.org/pp/draft_pps/	Publication expected Q4 2012
NIST SP 800-37	*National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 1.* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf	February 2010
NIST SP 800-38A	*National Institute of Standards and Technology (NIST) Special Publication (SP) 800-38A, Recommendation for Block Cipher Modes of Operation.* M. Dworkin. *http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf*	December 2001
NIST SP 800-38C	*National Institute of Standards and Technology (NIST) Special Publication (SP) 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality.* M. Dworkin. *http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf*	May 2004
NIST SP 800-38D	*National Institute of Standards and Technology (NIST) Special Publication (SP) 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* M. Dworkin. http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf	November 2007
NIST SP 800-53	*NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 3.* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf	August 2009
NIST SP 800-56A	*NIST Special Publication 800-56A. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.* E. Barker, D. Johnson, and M. Smid. http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf	March 2007
NIST SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion.* L. Chen. http://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf	November 2011
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 2246	*RFC 2246 The TLS Protocol Version 1.0.* T. Dierks and C. Allen. http://www.ietf.org/rfc/rfc2246.txt	January 1999
RFC 2407	*RFC 2407 The Internet IP Security Domain Interpretation for ISAKMP.* D. Piper. http://www.ietf.org/rfc/rfc2407.txt	November 1998
RFC 2408	*RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP).* D. Maughan, et.al. http://www.ietf.org/rfc/rfc2408.txt	November 1998

RFC 2409	*RFC 2409 The Internet Key Exchange (IKE).* D. Harkins and D. Carrel. http://www.ietf.org/rfc/rfc2409.txt	November 1998
RFC 2865	*RFC 2865 Remote Authentication Dial In User Service (RADIUS).* C. Rigney, et.al. http://www.ietf.org/rfc/rfc2865.txt	June 2000
RFC 3579	*RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP).* B. Aboba and P. Calhoun. http://www.ietf.org/rfc/rfc3579.txt	September 2003
RFC 3647	*RFC 3647 Internet X.509 Public Key infrastructure Certificate Policy and Certification Practices Framework Internet Engineering Task Force*. S. Chokhani, et.al. http://www.ietf.org/rfc/rfc3647.txt	November 2003
RFC 4106	*RFC 4106 The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP).* J. Viega and D. McGrew. http://www.ietf.org/rfc/rfc4106.txt	June 2005
RFC 4252	*RFC 4252 The Secure Shell (SSH) Authentication Protocol.* T. Ylonen and C. Lonvick. http://www.ietf.org/rfc/rfc4252.txt	January 2006
RFC 4253	*RFC 4253 The Secure Shell (SSH) Transport Layer Protocol.* T. Ylonen and C. Lonvick. http://www.ietf.org/rfc/rfc4253.txt	January 2006
RFC 4254	*RFC 4254 The Secure Shell (SSH) Connection Protocol.* T. Ylonen and C. Lonvick. http://www.ietf.org/rfc/rfc4254.txt	January 2006
RFC 4301	*RFC 4301 Security Architecture for the Internet Protocol.* S. Kent and K. Seo. http://www.ietf.org/rfc/rfc4301.txt	December 2005
RFC 4303	*RFC 4303 IP Encapsulating Security Payload.* S. Kent. http://www.ietf.org/rfc/rfc4603.txt	December 2005
RFC 4307	*RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).* J. Schiller. http://www.ietf.org/rfc/rfc4607.txt	December 2005
RFC 4308	*RFC 4308 Cryptographic Suites for IPsec.* P. Hoffman. http://www.ietf.org/rfc/rfc4608.txt	December 2005
RFC 4492	*RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, et.al. http://www.ietf.org/rfc/rfc4492.txt	May 2006
RFC 4868	*RFC 4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec.* S. Kelly and S. Frankel. http://www.ietf.org/rfc/rfc4868.txt	May 2007
RFC 5216	*RFC 5216, The EAP-TLS Authentication Protocol.* D. Simon, B. Adoba, and R. Hurst. http://www.ietf.org/rfc/rfc5216.txt	March 2008
RFC 5246	*RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2.* T. Dierks and E. Rescorla. http://www.ietf.org/rfc/rfc5246.txt	August 2008
RFC 5280	*RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* D. Cooper, et.al. http://www.ietf.org/rfc/rfc5280.txt	May 2008
RFC 5289	*RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM).* E. Rescorla. http://www.ietf.org/rfc/rfc5289.txt	August 2008
RFC 5903	*RFC 5903 Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2.* D. Fu and J. Solinas. http://www.ietf.org/rfc/rfc5903.txt	June 2010
RFC 5996	*RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2).* C. Kaufman, et.al. http://www.ietf.org/rfc/rfc5596.txt	September 2010

RFC 6379	*RFC 6379 Suite B Cryptographic Suites for IPsec.* L. Law and J. Solinas. http://www.ietf.org/rfc/rfc6379.txt	October 2011
RFC 6460	*RFC 6460 Suite B Profile for Transport Layer Security (TLS).* M. Salter, et.al. http://www.ietf.org/rfc/rfc6460.txt	January 2012

APPENDIX A CAMPUS WLAN ARCHITECTURE AND CONFIGURATION REQUIREMENTS

Capability Packages provide architecture and configuration information that allow customers to select COTS products from CSfC component lists for their solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data. CSfC component lists consist of eligible COTS products identified by model/version numbers that have met appropriate Protection Profile requirements.

This appendix contains requirements applicable to the Campus WLAN solution components. Several different kinds of requirements are provided: Architectural, Functional, and Configuration Guidance.

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

The products that are approved for use in this solution are listed on the IAD/CSfC website. No single commercial product shall be used to protect classified information. The only approved methods for using COTS products to protect classified information in transit on a Campus WLAN follow the requirements outlined in this Capability Package.

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

The requirement priorities are specified based on guidance contained in Section 2.1.1 of the Defense Acquisition Handbook. Based on this guidance, the “Threshold or Objective” column in each table means the following:

- An objective (O) requirement specifies a feature or function that the Government desires and expects.
- A threshold (T) requirement specifies a minimum acceptable feature or function that, in the Government’s judgment, still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to lack of technology maturity or time constraints).

In many cases, the threshold requirement also serves as the objective requirement (T=O). Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement complements the Threshold requirement rather than replaces it.

A.1 CSfC Overarching Requirements

Table A-1. Overarching Campus WLAN Architecture Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
	Vendor Diversity:		
PS.1	The Wireless System and VPN Gateway shall come from different vendors.	T=O	A
PS.2	The WLAN Authentication Server and VPN Gateway shall come from different vendors,	T=O	A
PS.3	The WLAN Client and the VPN Client shall come from different vendors	T=O	A
PS.4	One vendor cannot be a subsidiary of the other.	T=O	A
PS.5	The selection of components shall adhere to the restrictions shown in Table A-2.	T=O	A
PS.6	The WLAN and VPN CAs shall come from different vendors.	O	A
PS.7	**Hardware Platform Diversity:** On the Infrastructure side, the Wireless System, WLAN Authentication Server, and the VPN Gateway shall run on separate hardware platforms.	T=O	A
PS.8	**Operating System Environment**: On the Mobile Device, the IKE and WPA2 applications shall run as different operating system (OS) processes and use different cryptographic libraries.	T=O	A
PS.9	**Operating System (OS) Diversity:** The WLAN Controller and the VPN Gateway shall not utilize the same OS for critical IA security functionality. Differences between Service Packs (SP) or version numbers for a particular vendor's OS do not provide adequate diversity.	T=O	A
PS.10	The products selected for the Campus WLAN solution shall be from the CSfC Component List shown in Table A-3.	T=O	A

Table A-2. WLAN Solution Component Selection Restrictions

T (Threshold) or O (Objective) = indicates that the two components cannot originate from the same manufacturer. NOTE: This chart applies to purely commercial products. This chart does not apply to high assurance (Type-1) product vendors.	VPN Client	WLAN Client	VPN Gateway	Wireless System	WLAN Authentication Server	WLAN CA	VPN CA
VPN Client		T		T	T		
WLAN Client	T		T				
VPN Gateway		T		T	T		
Wireless System	T		T				
WLAN Authentication Server	T		T				
WLAN CA							O
VPN CA						O	

Table A-3. Applicable CSfC Component Lists for the Campus WLAN Solution

Component	CSfC Component List
Wireless System	Wireless System
WLAN Client	WLAN Client
WLAN Authentication Server	Authentication Server
WLAN Certificate Authority	Certificate Authority
VPN Gateway	IPsec VPN Gateway, Authentication Server
VPN Client	IPsec VPN Client
Firewall	Stateful Traffic Filter Firewall
Wireless Intrusion Detection System	See Appendix C

A.2 Configuration Requirements for the WLAN User Equipment (WUE)

If the WLAN UE OS provides robust key and certificate storage capabilities, it is acceptable to use the OS key and certificate store for both the WLAN and VPN clients. However, each client must be able to select the correct private key for authenticating itself and the correct root key certificate for validating certificates received from the WLAN Authentication Server and VPN Gateway. Accordingly, key storage and selection requirements are divided among the WUE, WLAN Client (WC), and VPN Client (VC) sections.

Table A-4. WLAN User Equipment (WUE) Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WUE.01	The WLAN UE shall be configured to associate only with authorized WLANs identified by Service Set Identifier (SSID).	O	C
WUE.02	The WLAN UE shall restrict configuration (SSID and authentication mechanism) of authorized WLANs to authorized administrators.	O	C
WUE.03	The WLAN UE shall comply with all security policies, directives, instructions, and requirements applicable to the system accessed by the WLAN.	O	C
WUE.04	The WLAN UE shall support administrative and user roles with separate authentication and privileges.	O	C
WUE.05	The WLAN UE shall be loaded with only approved software.	O	C
WUE.06	The WLAN UE shall restrict installation and removal of software to authorized administrators.	O	C
WUE.07	The WLAN UE shall audit critical security events (such as login, logout, key unlock, signature verification, certificate validation, decryption/integrity errors, installation and removal of software, changes to security-relevant configuration items).	O	C
WUE.08	The WLAN UE shall require a user to log in prior to granting access to any UE functionality.	T=O	C
WUE.09	The WLAN UE shall be configured to limit the number of incorrect logins per a configurable period of time either by erasing the configuration and data stored on the device or by prohibiting login attempts for a configured period of time.	T=O	C
WUE.10	The WLAN UE shall lock the screen and require user re-authentication after a configurable period of inactivity.	T=O	C
WUE.11	The WLAN UE shall display WLAN and VPN secure connection status information.	T=O	C
WUE.12	The WLAN UE shall be managed only on the enterprise network accessible via the Campus WLAN.	T=O	C
WUE.13	The WLAN UE shall interact with application services only on the enterprise network accessible via the Campus WLAN. Specifically, applications on the WLAN UE shall not be configured to access other networks.	T=O	C
WUE.14	The WLAN UE shall be configured such that WLAN and VPN encryption services cannot be bypassed.	O	C
WUE.15	The WLAN UE shall be configured such that WLAN and VPN services cannot be disabled.	O	C
WUE.16	The WLAN UE shall be configured to store private keys and their corresponding ITU-T X.509v3 certificates.	T=O	C
WUE.17	The WLAN UE shall be configured to store ITU-T X.509v3 certificates corresponding to trusted root CAs.	T=O	C

Table A-4. WLAN User Equipment (WUE) Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WUE.18	Any built-in, pre-loaded, or previously trusted loaded CA records, excepting those necessary for updates by the vendors, shall be deleted from the WLAN UE before introducing it to the architecture.	O	C
WUE.19	The WLAN UE shall be configured to protect the confidentiality and integrity of stored private keys using an auxiliary password of configurable length and complexity.	O	C
WUE.20	The WLAN UE shall be configured to protect the integrity of root key certificates using an auxiliary password of configurable length and complexity.	O	C
WUE.21	The WLAN UE shall not contain any self-signed or proprietary device certificates that are frequently preinstalled by the vendor.	O	C
WUE.22	The WLAN UE shall provide the capability to disable all wireless capabilities with the exception of WiFi.	T=O	C
WUE.23	The WLAN UE shall provide a notification if any wireless capability with the exception of WiFi has been enabled by the user.	O	C
WUE.24	The WLAN UE shall be configured to disable all unnecessary wireless capabilities excepting WiFi.	T=O	C
WUE.25	The WLAN UE shall provide Full Disk Encryption (FDE) or an equivalent capability.	O	C
WUE.26	The WLAN UE shall have a firewall configured according to organizational and local system policy.	O	C
WUE.27	The WLAN UE firewall shall be configured to allow only IKE, IPsec, and WPA2 authentication traffic.	O	C
WUE.28	The WLAN UE shall provide a hardware root of trust, trusted boot, and attestation that interoperates with the infrastructure to support remote assessment of integrity and compliance status.	O	C
WUE.29	The WLAN UE shall be configured with a monitoring service that detects unusual conditions or improper changes to configuration.	O	C
WUE.30	The WLAN UE shall be configured to use host-based security services (anti-virus, firewall, IDS).	O	C
WUE.31	The WLAN UE shall include tamper detection technology that provides evidence to end-users that unauthorized hardware modifications may have been performed (e.g., tamper seals).	T=O	C

A.3 Configuration Requirements for the WLAN Client (WC)

Table A-5. WLAN Client (WC) Configuration Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WC.1	The WLAN Client shall use the interim algorithms defined in Table A-6.	T	C
WC.2	The WLAN Client shall use the full Suite B algorithms defined in Table A-7 by 1 October 2015.	O	C
WC.3	The WLAN Client shall be configured to operate in the WPA2 Enterprise mode using ITU-T X.509v3 machine certificates for authentication.	T=O	C
WC.4	The WLAN Client shall perform mutual authentication with the WLAN Authentication Service using EAP-TLS via IEEE 802.1X.	T=O	C
WC.5	The WLAN Client tunnel shall be established at machine start-up using an ITU-T X.509v3 machine certificate.	O	C
WC.6	The WLAN Client shall be configured to authenticate only specific servers through: a) Setting the client to accept only a WLAN Authentication Server certificate that has been signed by the WLAN trusted root Certificate Authority (i.e., verifying the signatures on the whole certificate chain come from the trusted source); or b) Setting the client to accept only a WLAN Authentication Server certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	T	C
WC.7	The WLAN Client shall be configured to authenticate only specific servers through: a) Setting the client to accept only a WLAN Authentication Server certificate that has been signed by the WLAN trusted root Certificate Authority (i.e., verifying the signatures on the whole certificate chain come from the trusted source); and b) Setting the client to accept only a WLAN Authentication Server certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	O	C
WC.8	The WLAN Client shall be configured with a unique signature private key and corresponding ITU-T X.509v3 certificate.	T=O	C
WC.9	The WLAN Client shall use the unique signature private key for authenticating to the WLAN Authentication Server.	T=O	C
WC.10	The WLAN Client shall provide the user with advance warning that the WLAN client certificate is due to expire.	O	C

Table A-5. WLAN Client (WC) Configuration Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WC.11	The WLAN Client shall use the either the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ciphersuite (for TOP SECRET (TS) and below) or the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite (for SECRET (S) and below) with the WLAN Authentication Server.	T	C
WC.12	The WLAN Client shall use the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (for TS and below) ciphersuite or the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (for S and below) ciphersuite with the WLAN Authentication Server.	O	C
WC.13	The WLAN Client shall authenticate to the WLAN Authentication Server using an RSA digital signature.	T	C
WC.14	The WLAN Client shall authenticate to the WLAN Authentication Server using an ECDSA digital signature.	O	C
WC.15	The WLAN Client shall negotiate new session keys at least once per hour.	O	C
WC.16	The WLAN Client shall support Group Temporal Key (GTK) key encryption and integrity algorithms that are implementations of NIST AES Key Wrap with HMAC-SHA1-128 as specified in IEEE 802.11i.	T=O	C
WC.17	The WLAN Client shall be prevented from using ad hoc mode (client-to-client connections) and network bridging.	T=O	C
WC.18	The WLAN Client shall be configured to only associate with authorized SSIDs.	O	C
WC.19	Default accounts, passwords, community strings, and other default access control mechanisms for the administration of the WLAN Client shall be changed or eliminated.	T=O	C
WC.20	The WLAN Client shall verify that the WLAN Authentication Server X.509v3 certificate contains the TLS Web Server Authentication Object Identifier (id-kp-serverAuth 1.3.6.1.5.5.7.3.1) in the Extended Key Usage extension.	T=O	C

Table A-6. Approved Interim Algorithms

Security Service	Algorithm Suite (for TS and below)	Algorithm Suite (for S and below)	Specifications
Confidentiality (Encryption)	AES with 128 bits for WPA2 AES with 256 bits for VPN	AES with 128 bits	FIPS PUB 197
Authentication (Digital Signature)	WLAN Client: RSA (2048 bit modulus) with SHA-384 WLAN Authentication Server: ECDSA over the curve P-384 with SHA-384	RSA (2048 bit modulus) with SHA-1	FIPS PUB 186-3
Key Exchange/ Establishment	Ephemeral ECDH over the curve P-384 (DH Group 20)	Ephemeral 2048-bit Modular Exponentiation (DH Group 14)	NISP SP 800-56A IETF RFC 6379 IETF RFC 3526
Integrity (Hashing)	SHA-1	SHA-1	FIPS PUB 180-4

Table A-7. Approved Suite B Algorithms

Security Service	Algorithm Suite (for TS and below)	Algorithm Suite (for S and below)	Specification
Confidentiality (Encryption)	AES with 256 bits	AES with 128 bits	FIPS PUB 197
Authentication (Digital Signature)	ECDSA over the curve P-384 with SHA-384	ECDSA over the curve P-256 with SHA-256	FIPS PUB 186-3
Key Exchange/ Establishment	Ephemeral ECDH over the curve P-384 (DH Group 20)	Ephemeral ECDH over the curve P-256 (DH Group 19)	NIST SP 800-56A IETF RFC 6379 Suite B Cryptographic Suites for IPsec
Integrity (Hashing)	SHA-384	SHA-256	FIPS PUB 180-4

A.4 Configuration Requirements for the VPN Client (VC)

Table A-8. VPN Client (VC) Configuration Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
VC.1	The VPN Client shall use algorithms selected from Table A-6.	T	C
VC.2	The VPN Client shall use algorithms selected from Table A-7 by 1 October 2015.	O	C
VC.3	The VPN Client shall use IKEv1 with Phase 1 in Main Mode only (Aggressive Mode shall not be used) to perform authentication and key establishment (IKE).	T	C
VC.4	The VPN Client shall use IKE v2 to perform authentication and key establishment (IKE).	O	C
VC.5	The VPN Client shall use AES in Cipher Block Chaining (CBC) mode for IKE encryption.	T=O	C
VC.6	The VPN Client shall use AES in Cipher Block Chaining (CBC) mode for IPsec ESP tunnel-mode encryption.	T	C

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
VC.7	The VPN Client shall use AES Galois Counter Mode (GCM) for IPsec ESP tunnel-mode encryption.	O	C
VC.8	The VPN Client shall use an IKE SA lifetime of 24 hours.	T=O	C
VC.9	The VPN Client shall use an ESP SA lifetime of 8 hours.	T=O	C
VC.10	The VPN Client shall remove algorithm suites containing non-Suite B algorithms from the list of algorithms offered during negotiation.	O	C
VC.11	Default accounts, passwords, community strings, and other default access control mechanisms for the administration of the VPN Client shall be changed or eliminated.	T=O	C
VC.10	Any default, self-signed, or proprietary client certificates shall be removed.	T=O	C
VC.11	The VPN Client shall be configured to only authenticate specific servers through: a) Setting the client to accept only a VPN Gateway certificate that has been signed by the VPN trusted root Certificate Authority (i.e., verifying the signatures on the whole certificate chain come from the trusted source); or b) Setting the client to accept only a VPN Gateway certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	T	C

Table A-9. VPN Client (VC) Configuration Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
VC.12	The VPN Client shall be configured to only authenticate specific servers through: a) Setting the client to accept only a VPN Gateway certificate that has been signed by the VPN trusted root Certificate Authority (i.e., verifying the signatures on the whole certificate chain come from the trusted source); and b) Setting the client to accept only a VPN Gateway certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	O	C
VC.13	The VPN Client shall be configured with a unique signature private key and corresponding ITU-T X.509v3 certificate.	T=O	C
VC.14	The VPN Client shall use the unique signature private key for authenticating to the VPN Gateway.	T=O	C
VC.15	The VPN Client shall provide the user with advance warning that the VPN client certificate is due to expire.	O	C
VC.16	The VPN Client shall be configured to prohibit split tunneling.	O	C

A.5 Configuration Requirements for the WLAN System (WS)

The Wireless System is involved in establishing two encrypted channels. The first is a point-to-point IPsec tunnel-mode association with the WLAN Authentication Server for securely passing RADIUS attributes and the derived master session key. Once WLAN Authentication Server passes the master session key to the Wireless System, the Wireless System establishes an encrypted channel with the WLAN Client for passing data. The Wireless System acts as a pass-through for the initial authentication exchange between the WLAN Client and the WLAN Authentication Server during which the master session key is securely negotiated.

A.5.1 Wireless System Physical Configuration

Table A-9. Wireless System Configuration Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WS.1	The Wireless System shall be physically protected in accordance with the classification level of the system accessed by the Campus WLAN solution.	T=O	C
WS.2	The Wireless System shall not operate in the same spaces as an unclassified WLAN.	O	C

A.5.2 Wireless System to WLAN Client Interface

Table A-10. Wireless System to WLAN Client (WC) Client Interface Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WS.3	The Wireless System shall use the algorithms in Table A-6.	T	C
WS.4	The Wireless System shall use the algorithms in Table A-7 by 1 October 2015.	O	C
WS.5	The Wireless System shall be configured to operate in the WPA2 Enterprise mode (WPA2-Enterprise).	T=O	C
WS.6	The Wireless System shall act an EAP-TLS pass-through between the WLAN Client and WLAN Authentication Server for authentication and key establishment.	T=O	C
WS.7	The Wireless System shall negotiate new session keys with WLAN Clients at least once per hour.	T=O	C
WS.8	The Wireless System GTK key encryption and integrity algorithms shall be implementations of NIST AES Key Wrap with HMAC-SHA1-128 as specified in IEEE 802.11i.	T=O	C
WS.9	The Wireless System shall not broadcast multiple networks at different classification levels.	T=O	C

A.5.3 Wireless System to WLAN Authentication Server Interface

Table A-11. Wireless System to WLAN Authentication Server Interface Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WS.10	Communications between the Wireless System and the WLAN Authentication Server shall use the RADIUS protocol encrypted using point-to-point tunnel-mode IPsec.	T=O	C
WS.11	The IPsec key agreement shall use either IKEv1 with Phase 1 in Main Mode only (Aggressive Mode shall not be used) or IKEv2.	T=O	C
WS.12	The IKE protocol shall implement DH Group 2.	T	C
WS.13	The IKE protocol shall implement SHA-1 for integrity.	T	C
WS.14	The IPsec protocol shall implement SHA-1 for integrity.	T	C
WS.15	The IKE and IPsec protocols shall use the algorithms in Table A-7 by 1 October 2015.	O	C
WS.16	The IKE protocol shall implement AES in Cipher Block Chaining (CBC) mode.	T=O	C
WS.17	The IPsec protocol shall be ESP using AES in Cipher Block Chaining (CBC) mode.	T	C
WS.19	The IPsec protocol shall be ESP using AES in Galois Counter Mode (GCM).	O	C
WS.20	The IKE SA lifetime shall be set to 24 hours.	T=O	C
WS.21	The ESP SA lifetime shall be set to 8 hours.	T=O	C

Table A-12. Wireless System to WLAN Authentication Server Interface Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WS.22	The IKE protocol shall implement peer authentication using pre-shared keys or certificates.	T=O	C
WS.23	Composition rules for a pre-shared key shall be set by the Security Administrator.	T=O	C
WS.24	The estimated entropy of a pre-shared key shall be a minimum of 256 bits (for TS and below) or 128 bits (for S and below).	T=O	C
WS.25	Wireless systems authenticated by certificates shall be configured with a unique signature private key and corresponding ITU-T X.509v3 certificate signed by the WLAN CA.	T=O	C

A.6 Configuration Requirements for the Firewall (FW) Enclave

The Firewall Enclave is composed of a router configured with access control lists (ACLs) and a traditional network firewall appliance capable of deep packet inspection (DPI). The system ensures that the traffic flowing to and from each component on the network is appropriate for the functionality of the component within the Campus WLAN solution.

Table A-12. Firewall (FW) Enclave Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
FW.1	The Firewall Enclave shall contain two components, a traditional firewall capable of DPI and a screening router configured with ACLs.	T=O	A
FW.2	The screening router shall have only three interfaces in service, RI_OUT that connects to the wireless system, RI_IN that connects to the firewall appliance's outside interface (FWI_OUT), and RI_MAN for management of the router. All other interfaces shall be disabled.	T=O	C
FW.3	The screening router shall be configured to route only sessions entering the RI_OUT interface if the source address contained in the packet is one that is assigned by or owned by the WLAN system, the destination address is that of the VPN Gateway or the WLAN Authentication Server, and the destination port or protocol is necessary to the initiation and maintenance of the IPsec tunnel, including but not limited to ports 500 and 4500 User Datagram Protocol (UDP) and protocol 50 (ESP).	T=O	C

Table A-13. Firewall (FW) Enclave Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
FW.4	The screening router shall be configured to route only sessions entering the RI_IN interface if the source address is that of the VPN Gateway or the WLAN Authentication Server, the destination address contained in the packet is one that is assigned by or owned by the WLAN system, and the destination port or protocol is necessary to the initiation and maintenance of the IPsec tunnel, including but not limited to ports 500 and 4500 UDP and protocol 50 (ESP).	T=O	C
FW.5	The screening router shall deny and log all traffic not explicitly permitted.	T=O	C
FW.6	The firewall appliance shall have four interfaces, FWI_OUT that connects to the screening router's inside interface (RI_IN), FWI_DMZ1 that connects to the VPN Gateway, FWI_DMZ2 that connects to the WLAN Authentication Server, and FWI_MAN for the management of the firewall.	T=O	A
FW.7	The firewall appliance shall use static routes to route traffic. No dynamic routing protocols shall be used on the firewall.	T=O	C
FW.8	The firewall appliance shall permit the initiation of new sessions entering the FWI_OUT interface only if the source address contained in the packet is one that is assigned by or owned by the WLAN system, the destination address is that of the VPN Gateway or the WLAN Authentication Server, and the destination port or protocol is necessary to the initiation and maintenance of the IPsec tunnel, including but not limited to ports 500 and 4500 UDP and protocol 50 (ESP). All other new sessions entering the FWI_OUT interface will be denied.	T=O	C
FW.9	The firewall appliance shall deny all initiations of new sessions entering the FWI_DMZ1 and FWI_DMZ2 interfaces.	T=O	C
FW.10	The firewall appliance shall permit only established sessions entering the FWI_DMZ1 and FWI_DMZ2 interfaces.	T=O	C
FW.11	The firewall appliance shall deny and log all traffic not explicitly permitted.	T=O	C

A.7 Configuration of the VPN Gateway (VG)

Table A-13. VPN Gateway (VG) Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
VG.1	The VPN Gateway shall use algorithms selected from Table A-6.	T	C
VG.2	The VPN Gateway shall use algorithms selected from Table A-7 by 1 October 2015.	O	C
VG.3	The VPN Gateway shall use IKEv1 with Phase 1 in Main Mode only (Aggressive Mode shall not be used) to perform authentication and key establishment (IKE).	T	C
VG.4	The VPN Gateway shall use IKEv2 to perform authentication and key establishment (IKE).	O	C
VG.5	The VPN Gateway shall use ITU-T X.509v3 certificates for mutually authenticating the identities of the mobile device and VPN Gateway.	T=O	C
VG.6	The IKE SA lifetime shall be set to 24 hours.	T=O	C
VG.7	The ESP SA lifetime shall be set to 8 hours.	T=O	C
VG.8	The packet size for packets leaving the external interface of the VPN device shall be configured to minimize fragmentation.	T=O	C
VG.9	The proposals offered in the course of establishing the IKE Security Association (SA) and the ESP SA for the VPN shall be configured to offer algorithm suite(s) containing only interim algorithms (see Table A-6).	T	C
VG.10	The proposals offered in the course of establishing the IKE Security Association (SA) and the ESP SA for the VPN shall be configured to offer algorithm suite(s) containing only Suite B algorithms (see Table A-7).	O	C
VG.11	Algorithm suites containing non-interim algorithms or parameters shall be removed from the list of algorithms offered during negotiation (see Table A-6).	T	C
VG.12	Algorithm suites containing non-Suite B algorithms or parameters shall be removed from the list of algorithms offered during negotiation (see Table A-7).	O	C
VG.13	The VPN Gateway shall use AES in Cipher Block Chaining (CBC) mode for IKE encryption.	T=O	C
VG.14	The VPN Gateway shall use AES in Cipher Block Chaining (CBC) mode for IPsec ESP tunnel-mode encryption.	T	C
VG.15	The VPN Gateway shall use AES Galois Counter Mode (GCM) for IPsec ESP tunnel-mode encryption.	O	C
VG.16	The VPN Gateway shall be configured to restrict the IP address range for the network administration device to the smallest range possible.	T=O	C
VG.17	Default accounts, passwords, community strings, and other default access control mechanisms for the administration of the VPN Gateway shall be changed or eliminated.	T	C

Table A-14. VPN Gateway (VG) Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
VG.18	The default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, shall not be used for establishing SAs.	T	C
VG.19	The default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, shall be removed.	O	C
VG.20	A unique device certificate shall be loaded onto each VPN device along with the corresponding CA (signing) certificate.	T=O	C
VG.21	The device certificate shall be used for device authentication during IKE.	T=O	C
VG.22	The private key shall be stored on the VPN device and shall not be accessible through any of the non-management interfaces.	T=O	C
VG.23	The VPN Gateway shall be configured to prohibit split tunneling.	T=O	C
VG.24	The VPN Gateway shall be configured to audit and log when unauthorized access attempts and/or privilege escalation occur or are identified.	T=O	C
VG.25	The time of day on the VPN Gateway shall be synched with the Administration device and CA on the Enterprise network. This is necessary to ensure that certificates are accepted by the VPN device and to ensure adherence to the validity period of the certificate.	T=O	C
VG.26	The external interface of the VPN Gateway shall drop all packets that use IP options (e.g., if the first byte is not 0x45 for IPv4, then the packet shall be dropped and may be audited).	T=O	C
VG.27	The use of at least one outer interface loopback address is recommended. When present, the VPN Gateway's loopback address shall be used as the source address for management functions. This is advantageous instead of handling the numerous physical interface addresses.	T=O	C
VG.28	The VPN Gateway shall not store passwords for administrative access as plaintext.	T=O	C
VG.29	The VPN Gateway shall validate the VPN Client's X.509v3 machine certificate and check revocation information.	T=O	C
VG.30	The VPN Gateway shall validate the Distinguished Name or Subject Alternate Name in the VPN Client's X.509v3 machine certificate against a database of approved devices.	T=O	C
VG.31	The VPN Gateway shall trust only the VPN CA used within the solution.	T=O	C
VG.32	The VPN Gateway shall be configured with a valid VPN CA CRL either by retrieving the CRL or by manually installing the CRL when the previous CRL expires.	T=O	C
VG.33	Any built-in, pre-loaded, or previously trusted loaded Certificate Authority records, excepting those necessary for updates by the vendor, shall be deleted from the Gateway before introducing it to the architecture.	O	C

A.8 Configuration Requirements for the WLAN Authentication Server

The WLAN Authentication Server establishes a TLS tunnel with the WLAN Client for the purpose of authentication and to perform key negotiation to derive a shared session key (i.e., the Pair-wise Master Key (PMK) of the IEEE 802.11 standard) which is later passed to the Wireless System. It also establishes an IPsec VPN with the Wireless System to securely pass RADIUS attributes and the PMK.

A.8.1 WLAN Authentication Server to WLAN Client Interface

Table A-14. WLAN Authentication Server to WLAN Client Interface Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WAS.1	The WLAN Authentication Server and the WLAN Client shall perform EAP-TLS mutual authentication with ITU-T X.509v3 certificates using IEEE 802.1X as the authentication mechanism.	T=O	C
WAS.2	The WLAN Authentication Server shall disallow any authentication methods other than EAP-TLS.	T=O	C
WAS.3	A unique machine certificate corresponding to a private key shall be loaded into the WLAN Authentication Server along with the corresponding CA (signing) certificate. The certificate shall be used for machine authentication.	T=O	C
WAS.4	The WLAN Authentication Server shall send a certificate request to the WLAN Client and then validate the WLAN Client certificate and check revocation information.	T=O	C
WAS.5	The WLAN Authentication Server shall be configured with a valid WLAN CA CRL either by retrieving the CRL or by manually installing the CRL when the previous CRL expires.	T=O	C
WAS.6	The certificate shall contain the extendedKeyUsage field indicating support for Server Authentication (Object Identifier (OID) 1.3.6.1.5.5.7.3.1).	T=O	C
WAS.7	The WLAN Authentication Server shall additionally verify that the client certificate presented includes the Client Authentication purpose (OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.	T=O	C
WAS.8	Any built-in, pre-loaded, or previously trusted loaded Certificate Authority records, excepting those necessary for updates by the vendor, shall be deleted from the server before introducing it to the architecture.	O	C
WAS.9	The WLAN Authentication Server shall use the either the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (for TS and below) ciphersuite or the TLS_RSA_WITH_AES_128_CBC_SHA (for S and below) ciphersuite with the WLAN Client.	T	C

Table A-15. WLAN Authentication Server to WLAN Client Interface Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WAS.10	The WLAN Authentication Server shall use the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (for TS and below) ciphersuite or TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (for S and below) ciphersuite with the WLAN Client.	O	C
WAS.11	The WLAN Authentication Server shall validate the Distinguished Name or Subject Alternate Name in the WLAN Client's ITU-T X.509v3 machine certificate against a database of approved devices.	T=O	C

A.8.2 WLAN Authentication Server to Wireless System Interface Requirements

Table A-15. WLAN Authentication Server to Wireless System Interface Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WAS.12	Communications between the WLAN Authentication Server and the Wireless System shall use RADIUS encrypted using point-to-point tunnel-mode IPsec.	T=O	C
WAS.13	The key agreement shall use either IKEv1 with Phase 1 in Main Mode only (Aggressive Mode shall not be used) or IKEv2.	T=O	C
WAS.14	The IKE protocol shall implement DH Group 2.	T	C
WAS.15	The IKE protocol shall implement SHA-1 for integrity.	T	C
WAS.16	The IPsec protocol shall implement SHA-1 for integrity.	T	C
WAS.17	The IKE and IPsec protocols shall use the algorithms in Table A-7 by 1 October 2015.	O	C
WAS.18	The IKE protocol shall implement AES Cipher Block Chaining (CBC) mode.	T=O	C
WAS.19	The IPsec protocol shall be ESP using AES in Cipher Block Chaining (CBC) mode.	T	C
WAS.20	The IPsec protocol shall be ESP using AES in Galois Counter Mode (GCM).	O	C
WAS.21	The IKE SA lifetime shall be set to 24 hours.	T=O	C
WAS.22	The ESP SA lifetime shall be set to 8 hours.	T=O	C
WAS.23	The IKE protocol shall implement peer authentication using pre-shared keys or certificates.	T=O	C
WAS.24	Composition rules for a pre-shared key shall be set by the Security Administrator.	T=O	C
WAS.25	The estimated entropy of a pre-shared key shall be a minimum of 256 bits (for TS and below) or 128 bits (for S and below).	T=O	C

WAS.26	WLAN Authentication Servers authenticating to the Wireless System using certificates shall be configured with a unique signature private key and corresponding ITU-T X.509v3 certificate signed by the WLAN CA.	T=O	C

A.9 Configuration Requirements for Wireless Intrusion Detection System (WIDS)

Functional requirements for the Wireless IDS are defined in APPENDIX C.

Table A-16. Wireless IDS (WIDS) Configuration Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
WID.1	The WIDS shall be configured to require user identification and authentication for all administrative access to the system.	T=O	C
WID.2	The WIDS shall be configured to audit all administrative access and configuration changes to the system.	T=O	C
WID.3	The WIDS shall be configured to use HTTPS, SSH, or Secure File Transfer Protocol (SFTP) for remote event monitoring and for secure firmware/software updates.	T=O	C
WID.4	The WIDS shall be configured to authenticate and encrypt all communications with a remote administrator.	O	C
WID.5	The WIDS shall be configured with a whitelist of authorized access points and wireless clients.	T=O	C
WID.6	The WIDS shall be configured with a security policy that addresses, but is not limited to, detection of authorized devices operating on unauthorized channels, using an improper authentication method, using improper encryption, violating SSID cloaking policy, violating null SSID association policy, or establishing an ad hoc network.	T=O	C
WID.7	The WIDS shall be configured to detect unknown access points, including the provisioning WLANs, using a known SSID in the monitored area.	T=O	C
WID.8	The WIDS shall be configured to detect unauthorized clients attempting to connect to the authorized network.	T=O	C
WID.9	The WIDS shall be configured to detect authorized clients attempting to connect to unauthorized networks.	T=O	C
WID.10	The WIDS shall be configured to detect an authorized client connecting in two or more geographically different locations (such as buildings) simultaneously.	T=O	C
WID.11	The WIDS shall be configured with several wireless sensors in receive-only mode.	T=O	C
WID.12	The WIDS shall be configured to disable any active prevention techniques.	T=O	A

A.10 Configuration Requirements for Layer Separation in the Mobile Device

Table A-17. Cryptographic Module (CM) Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
CM.1	The VPN IKE Client and WLAN WPA2 Client shall be selected or configured to use different hardware cryptographic modules or software cryptographic libraries.	T=O	C
CM.2	The IPsec library and WLAN driver/adapter shall be selected or configured to use different cryptographic modules or software libraries.	T=O	C
CM.3	The cryptographic modules shall be configured to operate in FIPS-mode.	O	C

A.11 Configuration Change Detection (CCD) Requirements

Table A-18. Configuration Change Detection (CCD) Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
CCD.1	A baseline configuration for all devices shall be maintained.	T=O	C
CCD.2	An automated process shall ensure that configuration changes to the Wireless System, VPN Gateway, Firewall, WLAN Authentication Server, WLAN CA, and VPN CA are logged. This log entry shall include specific changes to the configurations.	T=O	C

A.12 Requirements for Infrastructure Device Administration (DA)

The requirements in this section apply to management and administration of infrastructure components. There are currently no requirements specified for Mobile Device Management (MDM).

Table A-19. Device Administration (DA) Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
DA.1	Management and administration of the VPN Gateway and other infrastructure components connected to the Enterprise network shall be performed from an administration device on the Enterprise network as follows and as illustrated in Figure A-1: • Administration of the VPN Gateway can be performed remotely over the Enterprise management network. If remotely administered, the SA shall use the SSH protocol as specified in RFCs 4252-4254, the IPsec protocol as specified in RFCs 2409, 4302, 4303, 4306, 4307, 4308, and 6379, or the TLS protocol as specified in RFCs 5246 and 6460.	T=O	C
DA.2	A separate LAN or Virtual LAN (VLAN) shall be deployed exclusively for managing and administering devices on the Enterprise network.	T=O	C/A
DA.3	Management and administration of the Wireless System, Firewall, WLAN Authentication Server, and other infrastructure components connected to the Mobility DMZ network shall be performed from an administration device on the Mobility DMZ network as follows and as illustrated in Figure A-1: • Administration of the Wireless System, Firewall, and WLAN Authentication Server can be performed remotely over the Mobility DMZ management network. If remotely administered, the SA shall use the SSH protocol as specified in RFCs 4252-4254, the IPsec protocol as specified in RFCs 2409, 4302, 4303, 4306, 4307, 4308, and 6379, or the TLS protocol as specified in RFCs 5246 and 6460.	T=O	C
DA.4	A separate LAN or VLAN shall be deployed exclusively for managing and administering devices on the Mobility DMZ network.	T=O	C/A
DA.5	The Admin workstations shall be properly configured according to local policy and U.S. Government guidance (e.g., Defense Information Systems Agency (DISA) gold disk, NSA guidelines). Adequate procedures shall exist for handling, storage, and lifecycle support. Antivirus software shall be running on all Admin workstations.	T=O	C

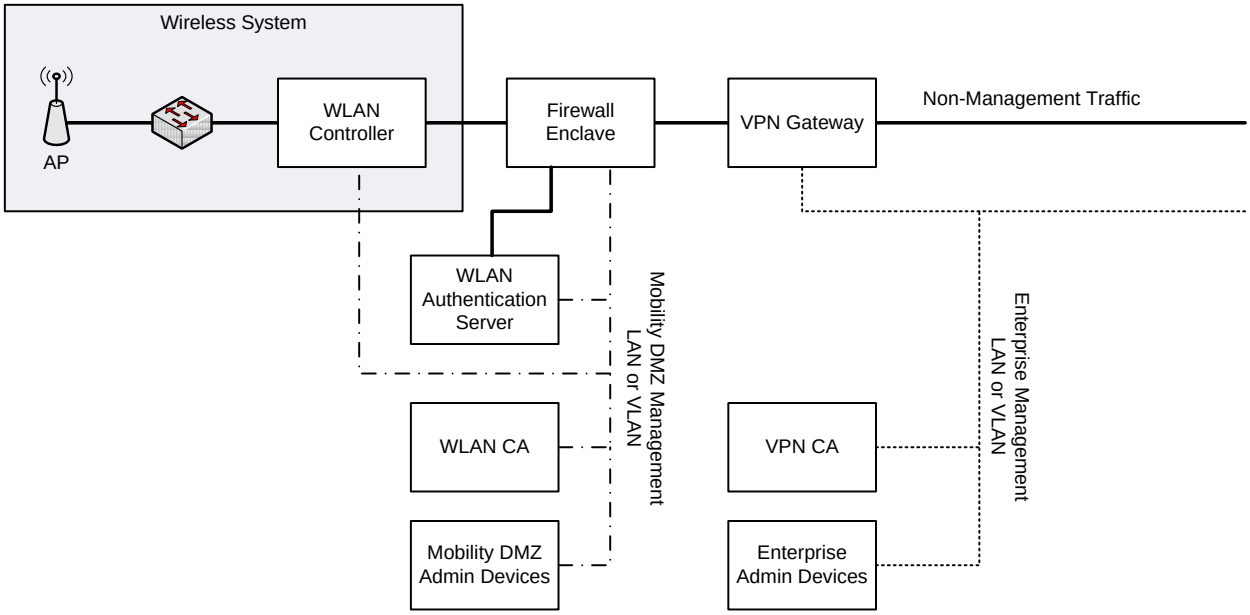

Figure A-1. Mobility DMZ and Enterprise Management Networks

A.13 Network Intrusion Detection System (NIDS) Requirements

Table A-20. Network Intrusion Detection System (NIDS) Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
IDS.1	A Network-based Intrusion Detection System (NIDS) shall be deployed on the Mobility DMZ Network to monitor traffic arriving from the Wireless System.	T=O	C/A
IDS.2	The NIDS shall report all potential intrusions.	T=O	C/A
IDS.3	The NIDS shall be regularly updated with attack signatures in accordance with local policy.	T=O	C

A.14 Requirements for Auditing (AU)

Table A-21. Auditing (AU) Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
AU.1	At a minimum, the following set of auditable events shall be logged by the infrastructure devices on a continuous basis: • All modifications to the audit configuration and all actions performed on the audit log (e.g., off-loading, deletion). • All actions involving identification and authentication. • Attempts to perform an unauthorized action (e.g., read, write, execute, delete) on an object. • All actions performed by a user with super privileges (e.g., auditor, administrator) and any escalation of user privileges. • Any changes to the baseline configuration of a product. • Certificate operations including generation, loading, or revoking of certificates. • Changes to time. • Receipt of unexpected data on any interface to the Mobility DMZ data or management networks (e.g., events logged by the screening router, firewall, or NIDS). • Any alerts or alarms logged by the WIDS. • All built-in self-test results, which may indicate failures in cryptographic functionality.	T=O	C
AU.2	The set of auditable events specified in the CPS shall be monitored and logged within the Wireless System, VPN Gateway, and WLAN Authentication Server on a continuous basis when in use.	T=O	C
AU.3	The following information shall be recorded for each audit event: • Date and time of the event. • Identifier for the event. • Type of event. • Success or failure of event to include failure code, when available. • Subject identity. • Source address for network based events. • User and role identification for role based events.	T=O	C

A.15 Requirements for PKI/Key Management (KM)

A.15.1 General PKI Requirements

Table A-22. General PKI Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
KM.1	The IPsec VPN and WLAN CAs shall issue ITU-T X.509v3 certificates.	T=O	C/A
KM.2	The IPsec VPN and WLAN CAs shall be located on separate networks (specifically, the Mobility DMZ management network for the WLAN tunnel devices and the Enterprise management network for the IPsec VPN tunnel devices).	T=O	C/A
KM.3	The IPsec VPN and WLAN CAs shall be members of different PKIs (i.e., have different root CAs).	T=O	C
KM.4	The IPsec VPN and WLAN CAs shall each operate under a CPS that is formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.	T=O	C
KM.5	The IPsec VPN and WLAN CAs shall initially key devices within a physical environment accredited to protect the highest classification level of data.	T=O	C
KM.6	The IPsec VPN and WLAN CAs shall rekey infrastructure devices prior to expiration of keys.	T=O	C
KM.7	The IPsec VPN and WLAN CAs shall update revocation information at the same time the device is rekeyed.	T=O	C
KM.8	The IPsec VPN and WLAN CAs shall not escrow private keys.	T=O	C
KM.9	The IPsec VPN and WLAN CAs are subject to audit requirements against the CPS.	T=O	C
KM.10	The IPsec VPN and WLAN CAs shall be properly configured according to local policy and U.S. Government guidance (e.g., DISA gold disk, NSA guidelines).	T=O	C
KM.11	The IPsec VPN and WLAN CAs shall run anti-virus software.	T=O	C
KM.12	The IPsec VPN and WLAN CAs shall issue certificates from a limited name space.	T=O	C
KM.13	The IPsec VPN and WLAN CAs shall generate a unique Distinguished Name (DN) in each certificate issued. (Note that the Common Name is not required to be unique.)	T=O	C
KM.14	The IPsec VPN and WLAN CAs shall assert a registered Object Identifier (OID) in the X.509v3 Certificate Policy extension.	T=O	C
KM.15	The IPsec VPN and WLAN CAs shall be chosen from the CSfC CA component list of NSA-approved CA devices. The Authorizing Official will need to approve the use of this CA, which will require a CP and CPS [RFC 3647].	T=O	C/A
KM.16	The IPsec VPN and WLAN CAs shall issue certificates with a validity period of no longer than 24 months.	T=O	C
KM.17	The IPsec VPN and WLAN CAs shall issue CRLs with a validity period of no longer than 30 days.	T=O	C

A.15.2 IPsec VPN PKI Requirements

Table A-23. IPsec VPN PKI Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
KM.18	The IPsec VPN CA shall support key sizes and algorithms as specified in Table A-6.	T	C
KM.19	The IPsec VPN CA shall support key sizes and algorithms as specified in Table A-7 by 1 October 2015.	O	C
KM.20	The IPsec VPN CA shall be a standalone CA located on the Enterprise network that is approved to issue Non-Person Entity (NPE) certificates to Edge devices or follows the same guidelines.	T	C
KM.21	The IPsec VPN CA shall be an approved Enterprise CA located on the Enterprise network that is approved to issue Non-Person Entity (NPE) certificates to Edge devices.	O	C/A
KM.22	The IPsec VPN CA shall post CRLs to a repository or service that is available to the VPN Gateway.	T=O	C/A
KM.23	The IPsec VPN CA shall be connected to the Enterprise management LAN or VLAN.	T=O	C/A

A.15.3 WLAN PKI Requirements

Table A-24. WLAN PKI Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
KM.23	The WLAN CA shall issue key sizes and algorithms as specified in Table A-6 and **Error! Reference source not found.**.	T	C
KM.24	The WLAN CA shall issue key sizes and algorithms as specified in Table A-7 by 1 October 2015.	O	C
KM.25	The WLAN CA shall issue certificates to the WLAN Authentication Server that contains the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage extension.	T=O	C
KM.26	The WLAN CA shall not issue certificates that contain the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage extension to any devices other than the WLAN Authentication Server and Wireless System.	T=O	C
KM.27	The WLAN CA shall issue certificates to WLAN Clients that contain the Client Authentication OID (1.3.6.1.5.5.7.3.2) in the ExtendedKeyUsage field. Reference is RFC 5216 EAP-TLS, Sect 5.3, March 2008.	T=O	C
KM.28	A standalone WLAN CA shall only issue certificates to WLAN Clients, the WLAN Authentication Server, the Wireless System, or to support its own operations.	T=O	C
KM.29	The WLAN CA shall issue only digital signature certificates to WLAN Clients.	T=O	C
KM.30	The WLAN CA shall post CRLs to a repository or service that is available to the WLAN Authentication Server.	T=O	C

KM.31	The WLAN CA shall be connected to the Mobility DMZ management LAN or VLAN.	T=O	C

A.16 Provisioning Requirements

A.16.1 Mobile Device Provisioning Requirements

Table A-25. Mobile Device Provisioning Requirements

Req #	Requirement Description	Threshold/ Objective	Architecture/ Configuration Guidance (A/C)
PR.1	A Provisioning WLAN using WPA2-PSK authentication and encryption shall be established on the Mobility DMZ network to support wireless provisioning of UEs.	T	A
PR.2	A Provisioning WLAN using WPA2-PSK authentication and encryption shall be established on the Enterprise network to support wireless provisioning of UEs.	T	A
PR.3	The Provisioning WLAN on the Mobility DMZ network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T	A
PR.4	The Provisioning WLAN on the Enterprise network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T	A
PR.5	UEs shall be provisioned over the Provisioning WLANs.	T	C/A
PR.6	UEs shall be provisioned over wired connections.	O	C/A
PR.6	When a UE has been successfully provisioned, its identity (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) shall be recorded in authorization databases accessible to the WLAN Authentication Server and VPN Gateway.	T=O	C/A
PR.7	It shall be possible to remove or disable UEs in the authorization database.	T=O	C/A
PR.8	The WLAN UE shall be loaded with an authorized software build during provisioning.	T=O	C
PR.9	The WLAN UE shall be loaded with WLAN and VPN configuration profiles during provisioning.	T=O	C
PR.10	The WLAN UE shall be provisioned by establishing password requirements, by disabling any unauthorized services, and by generating and/or loading of keys and certificates. (See separate key management requirements.)	T=O	C

APPENDIX B TEST CRITERIA

Test criteria will be supplied in a future version of this document.

APPENDIX C FUNCTIONAL REQUIREMENTS

Functional requirements for components without protection profiles are captured in this appendix. The component requirements for a WIDS (referred to in this appendix as "the system") are enumerated in this appendix as there is no CSfC component list or Protection Profile, existing or under development, for a WIDS.

C.1 WIDS General Requirements

Table C-1. WIDS General Requirements

Req #	Requirement Description	Threshold/ Objective
IDS-GEN.1	The WIDS shall provide secure remote system administration methods (Confidentiality, Integrity, and Availability) to ensure that all components of the system are in a known configuration and to provide the administrator with timely alerts.	T=O
IDS-GEN.2	The remote access administration shall be from the wired side and not from the wireless side.	T=O
IDS-GEN.3	The WIDS shall provide at least one method for secure remote event monitoring, including at least one of the following: HTTPS, SSH, or SFTP.	T=O
IDS-GEN.4	The WIDS shall provide at least one method for secure remote firmware/software updates, including at least one of the following: HTTPS, SSH, or SFTP.	T=O
IDS-GEN.5	The WIDS shall provide the ability to remove or disable all non-secure communications paths for system updates and event monitoring including, but not limited to, HTTP, SNMPv1, File Transfer Protocol (FTP), and Telnet over both wired and wireless transports. The preferred method is to completely remove these capabilities from the system.	T=O
IDS-GEN.6	The WIDS shall provide the ability to encrypt and authenticate all alerts pushed to a remote system administrator.	O
IDS-GEN.7	The WIDS shall monitor and indicate the health of the WLAN IDS and all of its individual components.	T=O
IDS-GEN.8	The WIDS shall generate, send, and log an alert whenever individual sensors and other IDS components fail to communicate.	T=O
IDS-GEN.9	The WIDS shall employ methods to ensure that the connections between all IDS components are secure. At a minimum, this shall include the use of FIPS certified encryption and two-way authentication.	T=O
IDS-GEN.10	In case an adversary tried to hide evidence of an attack in a flood of packets, the WIDS shall capture and parse all IEEE 802.11 traffic up to the maximum bit rate.	T=O
IDS-GEN.11	The system shall process every frame transmitted. In the event every frame is a malicious frame, the system shall not miss any alerts.	T=O
IDS-GEN.12	Wireless sensors shall be able to operate in receive-only (sensor) mode; they shall not transmit RF energy in the 2.4 GHz or 5 GHz IEEE 802.11 bands at any time, when in sensor mode.	T=O
IDS-GEN.13	WIDS monitoring components (i.e., sensors) shall not make wireless connections. Namely, sensors shall not make association requests or send association responses.	T=O

Table C-1. WIDS General Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective
IDS-GEN.14	The WIDS shall detect, log, and generate an alarm if any frames originate from a wireless sensor interface just as if it was any other unauthorized wireless device.	T=O
IDS-GEN.16	The WIDS shall provide the ability to filter alerts via the system Graphical User Interface (GUI).	T=O
IDS-GEN.17	The WIDS shall provide the ability to create custom filters based on a single or a combination of fields in the alert.	T=O
IDS-GEN.18	The WIDS shall associate events over an administrator adjustable time period, of at least one day, from anyone sensor and across multiple sensors.	T=O
IDS-GEN.19	The WIDS shall detect attacks and scans occurring over long periods of time.	T=O
IDS-GEN.20	The WIDS shall detect attacks and scans distributed throughout a network.	T=O
IDS-GEN.21	The WIDS shall provide the ability to import traffic collected from sources other than the system sensors and replay this traffic through the system detection engines. External sources may include, but are not limited to, tcpdump, Wireshark, or commercial capture products.	T=O
IDS-GEN.22	The WIDS shall provide cryptographically sound methods to verify that the sensor firmware and software has not been tampered with. The firmware/software integrity verification will apply when installing new firmware/software (i.e., hash values signed by the vendor's private key) as well as for periodic checks of all sensors.	T=O
IDS-GEN.23	The WIDS shall provide an automated method for verifying the firmware and software integrity of all sensors.	O
IDS-GEN.24	The WIDS shall provide cryptographically sound methods to verify that any WIDS-specific software on the computer(s) used to manage the system has not been tampered with.	O
IDS-GEN.25	To minimize false alarms, the WIDS shall provide the ability to selectively activate and deactivate the displaying of individual/unique alarms and events.	T=O

C.2 WIDS Physical Layer Analysis Requirements

Table C-2. WIDS Physical Layer Analysis Requirements

Req #	Requirement Description	Threshold/ Objective
IDS-PHY.1	The WIDS shall correctly determine the center frequency (channel) used for transmission for each frame received, not the frequency (channel) the receiver was on when the frame was captured.	O
IDS-PHY.2	The WIDS shall provide the ability to locate all authorized and unauthorized IEEE 802.11 wireless hardware operating in the IEEE 802.11 bands.	T=O
IDS-PHY.3	The WIDS shall log which sensor is closest to the wireless device.	T=O
IDS-PHY.4	The WIDS shall detect and log when it receives an IEEE 802.11 frame at a signal level substantially above the IEEE standard.	T=O
IDS-PHY.5	The WIDS shall detect and log RF-based denial-of-service attacks (DoS) (i.e., jamming, and interference).	T=O
IDS-PHY.6	The WIDS shall correlate the presence of new signals with a sudden increase in the frame error rate or a dramatic reduction in throughput, thus, indicating a potential attack.	O
IDS-PHY.7	The WIDS shall indicate the location of a logged device by using triangulation to locate the approximate position on a sensor map.	O

C.3 WIDS Frame Analysis Requirements

Table C-3. WIDS Frame Analysis Requirements

Req #	Requirement Description	Threshold/ Objective
IDS-FRA.1	The WIDS shall provide the ability to capture and store at a central location a single copy of each and every captured IEEE 802.11 frame, including Cyclic Redundancy Check (CRC) violations, regardless of the transmission frequency.	O
IDS-FRA.2	The WIDS shall provide the ability to store at least a week's worth of this data, to configure the lifetime of the captured data, and to create automatic backups and remote storage of the captured frames. The format of this stored data should be compatible with common protocol analyzers (e.g., comma-separated ASCII format).	O
IDS-FRA.3	The WIDS shall not drop any transmitted frames, including those frames with checksum errors or frames that violate the IEEE 802.11 standard.	T=O
IDS-FRA.4	The WIDS shall provide the ability to set up and configure filters to determine which captured frames are stored or forwarded to management computers.	T=O
IDS-FRA.5	The WIDS shall identify and log what sensor(s) captured a frame regardless of the frame's types and subtype.	T=O
IDS-FRA.6	The WIDS shall detect and log all violations of WLAN standards, including, but not limited to, IEEE 802.11 and IEEE 802.1X.	T=O
IDS-FRA.7	The WIDS shall detect and log when non-zero values appear in the reserved fields or when fields have atypical values.	T=O
IDS-FRA.8	The WIDS shall detect and log proprietary extensions to frames, such as additional information elements in beacons.	T=O

Table C-3. WIDS Frame Analysis Requirements (Cont.)

Req #	Requirement Description	Threshold/ Objective
IDS-FRA.9	The WIDS shall have the ability to detect and log undersized and oversized frames.	T=O
IDS-FRA.10	The WIDS shall provide the ability to tailor protocol anomaly signatures to fit individual needs. This entails the ability to create new attack signatures or to modify existing signatures.	O
IDS-FRA.11	The WIDS shall perform stateful frame inspection to detect and log attacks spanning multiple frames.	T=O
IDS-FRA.12	The WIDS shall detect anomalies, including, but not limited to, active probing, de-authentication and disassociation flooding, and RTS/CTS/NAK abuse.	T=O
IDS-FRA.13	The WIDS shall support user-defined intrusion events.	O
IDS-FRA.14	For the purpose of constructing custom signatures, the WIDS shall allow the administrator complete control over every field in an 802.11 frame and provide the ability to combine filters using the logical operators AND, OR, and NOT.	O
IDS-FRA.15	The WIDS shall detect and log deviations from the established network traffic baseline. It shall compute this baseline automatically, but the system administrator shall have the ability to override particular levels if desired.	O
IDS-FRA.16	If the network's activity deviates from a known profile, the WIDS shall use statistical analysis, also known as profile-based or anomaly detection, to generate an alarm.	O
IDS-FRA.17	The WIDS shall monitor specific network traits including, but not limited to, bandwidth usage, number of users/wireless clients, times of usage, user/wireless client location, and type of traffic.	O
IDS-FRA.18	In order for information in requirements IDS-FRA.16 and IDS-FRA.17 to be useful in determining usage patterns for each device and revealing deviations from normal patterns, the WIDS shall accumulate and analyze information over time. At least seven days of data shall be stored for this analysis.	O
IDS-FRA.19	The WIDS shall provide the administrator with the ability to set the length of time over which information is accumulated as identified in the above requirement.	O

C.4 WIDS Device Monitoring Requirements

Table C-4. WIDS Device Monitoring Requirements

Req #	Requirement Description	Threshold/ Objective
IDS-DEV.1	The WIDS shall track the connection status of each client (authorized or unauthorized) in real time including, but not limited to, whether the client is offline, associated, or authentication is pending.	T=O
IDS-DEV.2	The WIDS shall detect and log illegal state transitions, such as a client device transmitting data frames to a network device before being associated and authenticated.	T=O
IDS-DEV.3	The WIDS shall detect and log any unauthorized IEEE 802.11 transmitters operating in the area detectable by the sensors.	T=O
IDS-DEV.4	The WIDS shall detect and log any unauthorized clients attempting to connect to the wireless network.	T=O
IDS-DEV.5	The system shall distinguish between the mere existence of unauthorized hardware and an attempt to use that hardware to connect to the wireless network.	T=O
IDS-DEV.6	The WIDS shall detect and log any authorized clients associating to an unauthorized access point or communicating in ad-hoc mode with a client.	T=O
IDS-DEV.7	The WIDS shall detect and log an event where an attacker spoofs the MAC address of an authorized client.	T=O
IDS-DEV.8	The WIDS shall detect and log an event where two sensors in physically separate (non-overlapping) locations (such as different buildings) receive frames with the same MAC address at the same time.	T=O
IDS-DEV.9	The WIDS shall detect and log an event where a user's MAC address appears in multiple physically distant locations in too short a time span. The system shall provide the ability for the administrator to set the allowable time span and shall apply to both clients and access points.	O
IDS-DEV.10	The WIDS shall detect and log presence of two or more devices participating in an ad-hoc network or a device broadcasting beacons for an ad-hoc network.	T=O
IDS-DEV.11	The WIDS shall detect and log the presence of an IEEE 802.11 bridge, a single device transmitting beacons looking for a bridge, and/or two or more devices transmitting bridge data frames.	T=O
IDS-DEV.12	The WIDS shall support at least one configurable security policy. The security policy is defined by the system administrator and includes, but is not limited to, operating on unauthorized channels, using improper authentication methods, using improper encryption, violating SSID cloaking policy, or violating null SSID association policy.	T=O
IDS-DEV.13	The WIDS shall detect and log an authorized device's deviation from the security policy.	T=O
IDS-DEV.14	The WIDS shall detect and log unauthorized access points broadcasting with the same SSID as trusted access points.	T=O

APPENDIX D OPERATIONAL CONSIDERATIONS

D.1 Policy for the Use and Handling of Solutions

All implementing organizations using solutions to protect information on National Security Systems shall register their solutions with NSA prior to operational use. This registration will allow NSA to track where Campus IEEE 802.11 WLAN solutions are instantiated and to provide AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components approved for those solutions. The process for registering solutions is available on the CSfC web page (http://www.nsa.gov/ia/programs/csfc_program).

As with all computing/network resources, patches must be applied to Campus IEEE 802.11 WLAN solutions, and all Information Assurance Vulnerability Alerts (IAVAs) and/or Department/Agency security updates must be applied to the solution components. Configuration control of the solution over its lifecycle is an important function. If the solution is not properly updated, additional unanticipated/ unknown risks will be accepted by the AO if the solution continues to operate.

The following types of changes must be addressed during a component's/solution's lifecycle:

- Component Change: CSfC Components Lists and IA Alerts must be monitored for changes/updates. Guidance provided with the CSfC Components Lists and IA Alerts must be followed to continue to be in compliance with the Capability Package.
- Routine Capability Package Update: If a Capability Package is updated, all solutions based on that Capability Package must be validated against the latest Capability Package annually and have 6 months to come into compliance.
- Emergency Capability Package Update: If a Capability Package is deemed no longer to provide the level of security stated in the document, all solutions based on that Capability Package must be updated to the lasted version as soon as possible. NSA will provided an updated risk statement and possible mitigations (if available) to all registered users of the Capability Package with a required timeline for update.

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

P1. All components of the solution shall be physically protected as classified devices, classified at the level of the network in the solution with the highest classification. Only authorized and appropriately cleared (or escorted) administrators and security personnel should have physical access to the infrastructure components.

P2. The components of the CAMPUS IEE 802.11 WLAN solution do not provide any TEMPEST protections, thus any TEMPEST requirements should be met through the facility's environment, which should comply with local TEMPEST policy.

P3. All components of the solution should be disposed of as classified devices, unless declassified using procedures authorized by the AO.

P4. Acquisition and procurement documentation should not include information about how the equipment will be used, to include that it will be used to protect classified information.

P5. The solution owner should allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, and interviewing) of the solution implementation as determined by NSA.

P6. The Authorizing Official will ensure that a compliance audit should be conducted every year against the latest version of the Campus IEEE 802.11 WLAN Capability Package, and the results should be provided to the Authorizing Official.

P7. All components should be IAVA compliant and/or Department/Agency security updates must be applied to the solution components in accordance with local policy.

P8. Solution implementation information, which is provided to NSA during solution registration, should be updated every 12 (or fewer) months. (Registration allows NSA to track where Campus IEEE 802.11 WLAN solutions are instantiated and to provide Authorizing Officials at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components approved for those solutions.)

P9. Audit log data for security critical events (see Auditing requirements in Appendix A) should be handled according to the following requirements:

1. Audit logs should be reviewed by the Auditor at least monthly (or more frequently if required by the local Authorizing Official) to look for unauthorized access.
2. Audit log data should be maintained for a minimum of 1 year (or less if approved by the Authorizing Official).
3. During the monthly review of the audit data, the amount of storage remaining for audit events should be assessed in order to ensure that adequate memory space is available to continue recording new audit events.
4. Audit data should be frequently offloaded to a backup storage medium in order to facilitate compliance with requirements 2 and 3 above.

P10. A set of procedures should be developed to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.

P11. A procedure should be developed for ensuring continuity of operations for the auditing capability. This plan should include each of the following as a minimum:

1. A mechanism or method for determining when the audit log is reaching its maximum storage capacity.
2. A mechanism or method for off-loading audit log data for long term storage.
3. A mechanism or method for responding to an overflow of audit log data within a product.
4. A mechanism or method for ensuring that the audit log can be maintained during power events.

P12. Passwords—Strong passwords should be used that comply with the requirements of the local security authority.

P13. User policy:

1. Users should not establish a network or data connection from the mobile device to an Enterprise network other than through an authorized Campus WLAN connection.
2. Users should not change the administrator-configured settings of the device, including, but not limited to, the WLAN and VPN configurations, the wireless settings, the loaded software build, and the applied anti-tamper technologies.
3. Users should report loss, theft, deactivation, destruction, or suspected compromise (e.g., detected tamper) of devices in compliance with procedures established by the implementing organization.

P14. A set of procedures should be developed to provide guidance for securely provisioning and initializing devices. This plan should include each of the following as a minimum:

1. Identification of the policy for configuring devices.
2. Requirements to identify and authorize users and devices prior to provisioning.
3. Registration and configuration of devices.
4. Requesting, issuing, and loading of certificates and key material for devices.

P15. A set of procedures should be developed to provide guidance for managing device access to the WLAN. This plan should include each of the following as a minimum:

1. Identification of the databases and mechanisms used to authenticate and authorize access to the WLAN including the VPN Gateway.
2. Identification of the Certificate Policy/Certification Practice Statements for the WLAN and VPN CAs that specify the certificate validity period, CRL validity period, frequency of CRL issuance, and methods for revoking certificates.
3. Management of the registration/authorization databases.
4. Means for reporting and responding to loss, theft, deactivation, destruction, or suspected compromise (e.g., detected tamper) of devices including when to revoke certificates and delete devices from authorization databases and means to temporarily suspend access (if provided).
5. Policies for regular and random inspection of devices to detect loss, theft, and physical or technical compromise.

D.2 Role-Based Personnel Requirements

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

Security Administrator—The Security Administrator should be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the Campus IEEE 802.11 WLAN solution within a single site.

Security Administrator duties include but are not limited to:

1. Ensuring that the latest software patches and updates, to include IAVAs, are applied to each product.

2. Documenting and reporting security-related incidents to the appropriate authorities.
3. Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.
4. Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the Campus IEEE 802.11 WLAN Solution.
5. Ensuring that the implemented Campus IEEE 802.11 WLAN Solution remains compliant with the latest version of this Capability Package.
6. Monitoring the Wireless IDS logs on a regular basis (preferably full-time) to detect signs of attempted wireless intrusion attempts.
7. Denying access by UEs by removing their identities from the WLAN and VPN authorization databases. This duty may include coordinating with the Certificate Authority Administrator (CAA) to revoke certificates.

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

1. Administering the CA, including authentication of all devices requesting certificates.
2. Maintaining and updating the Certificate Revocation List.
3. Notifying the Security Administrator of revoked certificates so they can be removed from WLAN and VPN authorization databases.

Auditor—The Auditor should be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the Campus IEEE 802.11 WLAN Solution. The role of Auditor and Security Administrator should not be performed by the same individual. The Auditor should only be allowed access to the Mobility DMZ network and Enterprise network administration devices. Auditor duties include but are not limited to:

1. Reviewing, managing, controlling, and maintaining security audit log data.
2. Documenting and reporting security-related incidents to the appropriate authorities.

Solution Integrator—In certain cases, an external integrator may be hired to implement a Campus IEEE 802.11 WLAN Solution based on this Capability Package. Solution Integrator duties may include but are not limited to:

1. Acquiring the products that compose the solution.
2. Configuring the Campus IEEE 802.11 WLAN Solution in accordance with this Capability Package.

Additional policies related to the personnel that perform these roles in a Campus IEEE 802.11 WLAN Mobile Device Solution are as follows:

RB1: The Security Administrator, CAAs, Auditor, and all Solution Integrators should be cleared to the highest level of data protected by the Campus IEEE 802.11 WLAN solution.

RB2: When a previously established CA is utilized in the solution, the CAA already in place should also support this solution provided they meet RB1.

RB3: The Security Administrator, CAA, and Auditor roles should be performed by different people.

RB4: All Security Administrators, CAAs, and Auditors should meet local information assurance training requirements.

RB5: The CAA for the Enterprise network should be different from the CAA for the Mobility DMZ management network.

D.3 Information to Support Authorizing Official

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

- The implementing organization, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved Capability Package.
- The implementing organization has a testing team develop a Test Plan and perform testing of the Campus IEEE 802.11 WLAN Architecture solution, see APPENDIX B.
- The implementing organization has system certification and accreditation performed utilizing the risk assessment information referenced in APPENDIX D.
- The implementing organization provides the results from system certification and accreditation to the AO for use in making an approval decision.
- The implementing organization registers the solution with NSA and reregisters yearly to validate its continued use as detailed in APPENDIX D. The validation should include a review of the latest version of the Capability Package and associated Risk Assessment.

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

The risk assessment of the Campus IEEE 802.11 WLAN Solution presented in this Capability Package documents the threat, mitigations, residual risk, and potential countermeasures associated with the solution. To comply with this Capability Package, the AO much thoroughly review the risk assessment and determine that the residual risks are acceptable for the system implementing the solution. It is strongly recommended that others associated with integrating, administering, and auditing the system also review the risk assessment. The classified risk assessment document for the WLAN Architecture can be obtained by contacting the NSA/IAD Client Advocate for the implementing organization. The classified risk assessment document for the Campus IEEE 802.11 WLAN Solution is also available on the SIPRNet CSfC website.

D.4 High Level Description of a Mobile Device-Infrastructure Connection

The following summarizes the sequence of events that occur in order to establish network access from a wireless Mobile Device in the architecture:

1. The Mobile Device is powered on. The WLAN Client automatically associates with the Wireless System.
2. The Wireless System requires the WLAN Client to perform an IEEE 802.1X authentication before providing access. The WLAN Client and WLAN Authentication Server mutually authenticate using

ITU-T X.50v39 machine certificates. The Wireless System acts as a pass through to WLAN Authentication Server during these communications. If either WLAN Authentication Server or the WLAN Client determines that the other party's certificate is not valid, communication will cease.

3. The WLAN Client and WLAN Authentication Server execute a key establishment protocol (EAP-TLS) to derive the PMK.
4. WLAN Authentication Server passes the PMK to the Wireless System using RADIUS inside an IPsec protected wired connection. Depending on the vendor, the Wireless System will either keep the PMK on the Wireless Controller or push the keys out to the appropriate AP as needed.
5. The WLAN Client and Wireless System perform a 4-way handshake to derive a session key from the PMK. From this point forward all communication between the Wireless Client and the Wireless System is protected with this session key.
6. The VPN Client and VPN Gateway mutually authenticate via ITU-T X.509v3 machine certificates. If either the VPN Client or the VPN Gateway determines that the other party's certificate is not valid, all communications will cease.
7. The VPN Client and VPN Gateway negotiate keys, algorithms, and parameters for the IPsec connection using IKE. From this point forward all communication between the VPN Client and VPN Gateway is protected with an IPsec tunnel.
8. At this point the Mobile Device is connected to the wired network, but does not have access to services. Unless the system owner wants to establish a user authentication method specifically for wireless users, the Mobile Device and the network perform a user authentication to gain service access using the authentication method already implemented on the wired network.