CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Specification Access Network Connectivity

CMI-SP-F-ANC-D02-2019-05-31

Draft

Notice

This specification is the result of a cooperative effort undertaken at the direction of the Center for Medical Interoperability™ for the benefit of the healthcare industry and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by The Center in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by The Center. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open source licenses, if any.

DISCLAIMER

This document is furnished on an "AS IS" basis and neither The Center nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and The Center and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

The Center reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by The Center or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from The Center, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Table of Contents

Document Status Sheet

Document Control Number:	CMI-SP-F-ANC
Document Title:	Access Network Connectivity
Revision History:	D02 IPR Review
Date:	03/21/2019
Status:	Draft
Distribution Restrictions:	Public

Key to Document Status Codes

Work in Progress	An incomplete document designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document considered largely complete but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through The Center.

1 Scope

1.1 Introduction and Purpose

This specification documents The Center's wireless and wired access network connectivity requirements for medical devices and health care access networks. These requirements meet objectives for several stakeholder groups:

- **Health Care Provider Members of The Center:** With the standard wireless requirements documented here, health care providers can be assured that their wireless networks help meet the needs of the health care staff. Medical devices reliably connect to health care networks. Wireless connectivity and performance are consistent and predictable across medical facilities and regions. For wired portions of the network, this provides additional security requirements to ensure similar trust.
- **Vendors:** The access network requirements contained in this document provide vendors a minimum set of capability requests from numerous Health Care Provider customers across the health care industry. Vendors benefit from consistent behavior across member networks and in multi-vendor environments.
- **Consumers of Health Care:** Consumers may not necessarily interact directly with The Center specified access networks, but they benefit indirectly by the reliable use of connected medical devices.

Requirements are primarily twofold: wireless air interface, and security requirements for wired networks. Given the larger scope of wireless access networks, these are described in more detail and form a majority of this specification.

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"SHALL"	This word means that the item is an absolute requirement of this specification.
"SHALL NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 References

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

[CMI-SP-F-ID]	Identity https://medicalinteroperability.org/specifications
[CMI-SP-F-PF]	Provisioning Flows https://medicalinteroperability.org/specifications
[FCC-KDB-905462]	Test guidance for U-NII devices subject to the DFS requirements https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?switch=P&id=27155
[IEEE-802.11-2016]	IEEE 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 https://standards.ieee.org/standard/802_11-2016.html
[IEEE-802.1AE-2006]	IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security https://standards.ieee.org/standard/802_1AE-2006.html

[IEEE-802.1X-2010]	IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control https://standards.ieee.org/content/ieee-standards/en/standard/802_1X-2010.html
[IETF-RFC5246]	The Transport Layer Security (TLS) Protocol Version 1.2 https://tools.ietf.org/html/rfc5246
[IETF-RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://tools.ietf.org/html/rfc5280
[IETF-RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[WFA-Agile-1.2]	Wi-Fi Agile Multiband Specification Version 1.2 2018 https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_Agile_Multiband_Specification_v1.2.pdf/34975
[WFA-CERTIFIED-n]	Wi-Fi CERTIFIED n: Operates in both 2.4 and 5 GHz. Wi-Fi CERTIFIED n is still used today in many Internet of Things (IoT) devices, including wearables and smart televisions. https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-n
[WFA-Hotspot-2.0]	Wi-Fi Alliance: Hotspot 2.0 Release 2, 2014 https://www.wi-fi.org/downloads-registered-guest/Hotspot_2-0_%2528R2%2529_Technical_Specification_Package_v1-4_0.zip/29728
[WFA-WMM]	Wi-Fi Alliance: Wi-Fi Multi-Media QoS based on 802.11e, Version 1.1, 2012.
[WFA-WPA2]	Wi-Fi Alliance: Wi-Fi Protected Access (WPA) Enhanced Security Implementation Based on IEEE P802.11i standard, Version 3.1, August 2004.

2.2 Informative References

This specification uses the following informative references.

[CMI-DOC-TD]	Terms and Definitions https://medicalinteroperability.org/specifications
[CMI-ORG-TWH]	Trusted Wireless Health, Center for Medical Interoperability, Sept. 2018 https://medicalinteroperability.org/specifications/cmi-org-twh
[CMI-SP-CDI-IHE-PCD-IST]	Clinical Data Interoperability Based on IHE PCD – Identity & Secure Transport https://medicalinteroperability.org/specifications
[CMI-SP-F-CP]	Certificate Policy https://medicalinteroperability.org/specifications
[FIPS-140-2]	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[IEEE-802.11e-2005]	IEEE Standard for Information technology--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements https://standards.ieee.org/standard/802_11e-2005.html
[IEEE-802.11i-2004]	IEEE 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: Amendment 6: Medium Access Control (MAC) Security Enhancements https://standards.ieee.org/standard/802_11i-2004.html
[IEEE-802.11h-2003]	IEEE 802.11h-2003 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe https://standards.ieee.org/standard/802_11h-2003.html

[IEEE-802.11k-2008] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs

https://standards.ieee.org/standard/802_11k-2008.html

[IEEE-802.11n-2009] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput

https://standards.ieee.org/standard/802_11n-2009.html

[IEEE-802.11r-2008] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition

https://standards.ieee.org/standard/802_11r-2008.html

[IEEE-802.11u-2011] IEEE Standard for Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks-specific requirements-Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 9: Interworking with External Networks

https://standards.ieee.org/standard/802_11u-2011.html

[IEEE-802.11v-2011] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management

https://standards.ieee.org/standard/802_11v-2011.html

[IEEE-802.11w-2009] IEEE 802.11w-2009 - IEEE 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 Amendment 4: Protected Management Frames

https://standards.ieee.org/standard/802_11w-2009.html

2.3 Reference Acquisition

- Center for Medical Interoperability, 8 City Blvd, Nashville, TN 37209; https://medicalinteroperability.org

- Federal Communications Commission (FCC), 445 12th Street SW, Washington, DC 20554; https://www.fcc.gov
- Institute of Electrical and Electronics Engineers (IEEE), 3 Park Avenue, 17th Floor, New York, NY 10016-5997; https://www.ieee.org
- The Internet Engineering Task Force (IETF), IETF Secretariat®, c/o Association Management Solutions, LLC (AMS), 5177 Brandin Court, Fremont, CA 94538, USA; Phone: +1-510-492-4080; https://www.ietf.org
- National Institute for Standards and Technology (NIST), 100 Bureau Drive, Gaithersburg, MD 20899; Phone: +1-301-975-2000, https://www.nist.gov
- Wi-Fi Alliance, 10900-B Stonelake Boulevard, Suite 126, Austin, Texas 78759, https://www.wi-fi.org ; Wi-Fi®, Wi-Fi Alliance®, WMM®, Wi-Fi Certified™, W-Fi Protected Access®, WPA2™, Hotspot 2.0® and Passpoint® are trademarks of the Wi-Fi Alliance.

3 Terms and Definitions

This specification uses the terms and definitions in [CMI-DOC-TD].

4 Abbreviations and Acronyms

This specification uses the following abbreviations:

AAA	**Authentication, Authorization and Accounting**
ANQP	Access Network Query Protocol
AP	Access Point
ARP	Address Resolution Protocol
BSS	Basic Service Set
CA	Certification Authority
CEE	Cell Edge Environment
CHAP	Challenge Handshake Authentication Protocol
CRL	Certificate Revocation List
DFS	Dynamic Frequency Selection
DMZ	Demilitarized zone
EAPOL	Extensible Authentication Protocol over LAN
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ECC	Elliptic Curve Cryptography
EIRP	Estimated Isotropic Radiated Power
GAS	Generic Advertisement Service
HDO	Healthcare Delivery Organization
IKE	Internet Key Exchange
LAN	Local Area Network
MAC	Medium Access Control
MACsec	Media Access Control Security
NAI	Network Access Identifier
OCSP	Online Certificate Status Protocol

OI	Organizational Identifier
PER	Packet Error Rate
PHY	Physical layer
PKI	Public Key Infrastructure
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RF	Radio frequency
SINR	Signal to Interfering Noise Ratio
SSID	Service Set Identifier
STA	Station
U-NII	Unlicensed National Information Infrastructure
URL	Uniform Resource Locator
VLAN	Virtual LAN
WAC	Wi-Fi Access Controller
WAN	Wide Area Network
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity
WMM	Wi-Fi Multi-Media
WPA	Wi-Fi Protected Access

5 Wireless Access Network Overview

This section describes a high-level end-to-end architecture for medical devices that connect to Wi-Fi networks. Functional elements are identified and described. Access Network Connectivity Requirements specifies access network connectivity for components that connect to a health system's access network.

5.1 End-to-End Architecture

5.1.1 Hotspot 2.0 applied to Wi-Fi networks

Figure 1 illustrates the high-level Wi-Fi access network architecture for the health care system network.

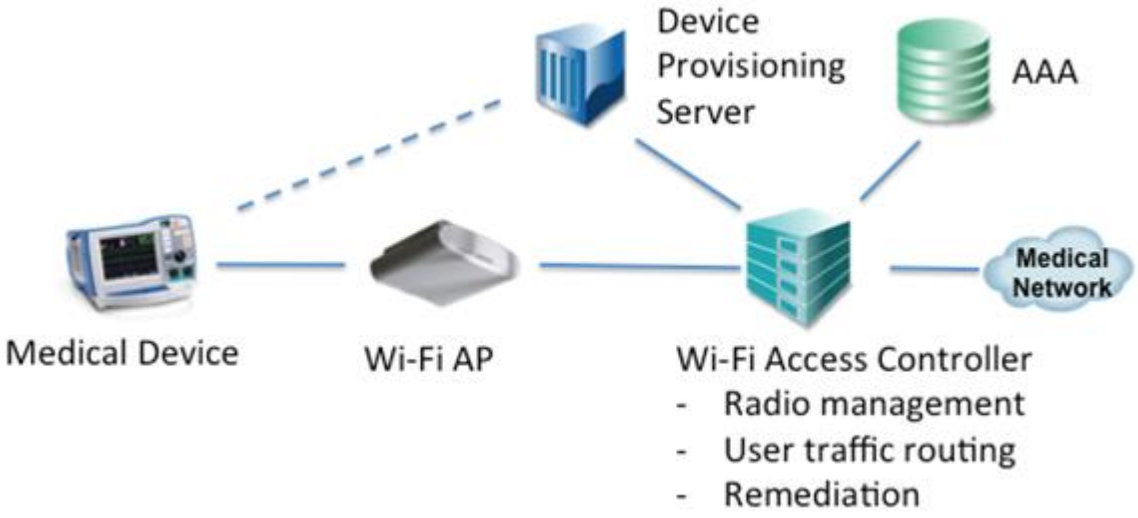

Figure 1 - Wi-Fi Access Network Architecture Diagram

A client (medical device) connects to the Wi-Fi AP over the specified air interface. Key capabilities on the AP air interface include high data rates, quality of service prioritization, enterprise security, fast transitions across APs, and automated network discovery and selection. The AP is controlled by the Wi-Fi Access Controller (WAC). The WAC provides radio resource management, user traffic routing and user access remediation. The Device Provisioning Server configures the Wi-Fi air interface on wirelessly connected components. Configuration encompasses RF settings, 802.11 settings, SSID profiles, subscriber profiles, security settings and network selection policy. The AAA provides authentication and authorization for admission of clients to the health care provider's Wi-Fi network. It can also be used to account for client usage of network resources. The AAA may hold the client's subscriptions to the health care wireless network, or interface to an external database that holds the subscriptions.

This specification focuses on requirements for the client. Health care providers and their vendors are free to implement the logical capabilities described herein for the WAC, Device Provisioning

Server, and AAA at various levels of integration. For example, the functions of the Wi-Fi Access Controller could be distributed across products or integrated into a single product with additional functions.

5.1.2 Backwards compatibility with WPA2 Enterprise

Hotspot 2.0 provides for automated Wi-Fi network discovery and selection per health care provider network policy. It is important to note that Hotspot 2.0 is fully backwards compatible with WPA2-Enterperise security. Legacy devices can attach to SSIDs that support Hotspot 2.0 without modification and use the same procedures as they would with conventional WPA2 enterprise SSIDs. This allows health care networks to migrate their medical devices to Hotspot 2.0 at a pace that meets the needs of the health organization.

5.2 Access Network Connectivity Flow

Figure 2 provides a high-level functional messaging flow for wireless access of a Hotspot 2.0 medical device to the health care network. This diagram does not portray protocol level messaging, but high-level functional concepts.

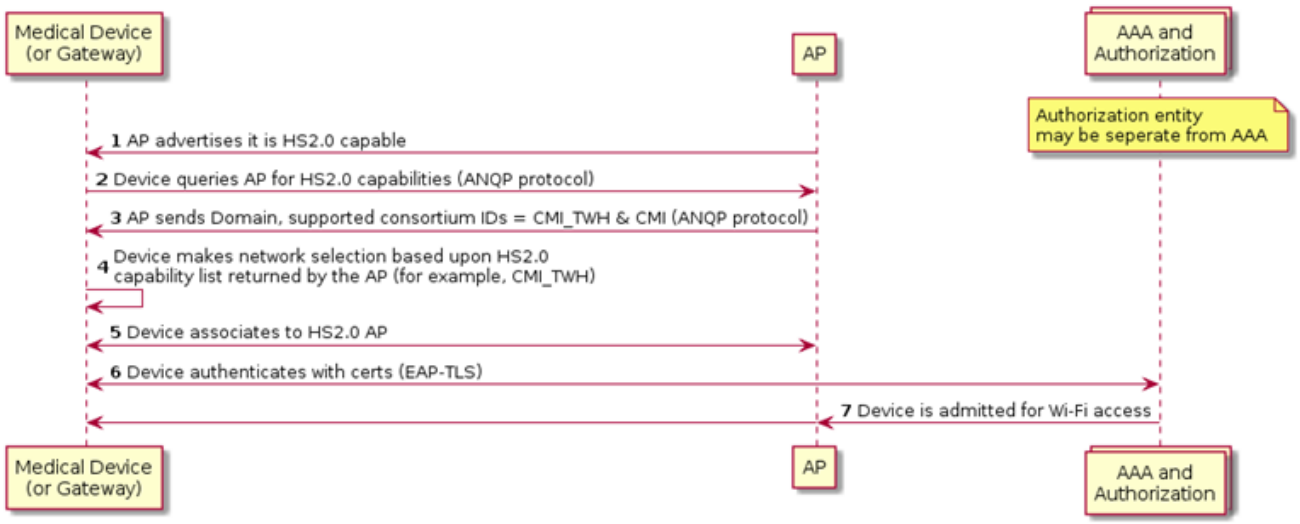

Figure 2 - High Level Functional Flow of Network Access

As shown in Figure 2, the Hotspot 2.0 AP advertises that it is Hotspot 2.0 capable per information elements as specified in [IEEE-802.11u-2011]. The Hotspot 2.0 device detects that the AP is Hotspot 2.0-capable, and then performs an Access Network Query Protocol (ANQP) query to the AP in order to retrieve the list of capabilities that the AP supports. Capabilities include operator support, roaming capabilities, authentication options, bands of operations and additional capabilities defined in Hotspot 2.0. In the third message of the flow, the AP indicates its roaming capability to support two network access identifiers (NAI), CMI_TWH and CMI, or their respective Roaming Consortium Organizational Identifiers. “CMI” indicates that the network is ready to receive CMI compliant devices. "CMI_TWH" indicates that the network supports Trusted Wireless Health [CMI-ORG-TWH] requirements. The device is configured to select the AP for association based upon the

preferred consortium OI or NAI "CMI_TWH". The device then starts the authentication process with a pre-configured WPA2-Enterprise profile for EAP-TLS with certificates. The device receives and authenticates the AAA server certificate. The AAA server authenticates the certificate received from the device and completes the mutual authentication process. The AAA server admits the device onto the secured Wi-Fi air interface as authorized by the medical network. The authorization process is not described in this document. Once the AP receives admission authorization from the AAA, it accepts the device onto the Wi-Fi access network and user traffic is secured over the air interface.

5.3 Access Network Design – Trusted Wireless Health

Trusted Wireless Health (TWH) [CMI-ORG-TWH] networks are tuned to ensure consistent, strong signals for many overlapping layers of traffic. TWH network design begins with an interlaced, geometric pattern and is comprehensively verified to ensure dense coverage throughout the space. These networks are built to enable symmetric communication between APs and STAs, limiting AP transmit power to 8 dBm and maintaining minimum signal levels of -63 dBm. Critically, the many layers of non-interfering wireless traffic allow HDOs to completely segregate guest traffic and greatly reduce airtime utilization on clinical networks. Many elements of this specification are intended to optimize device operation in TWH environments. For example, IEEE wireless roaming standards address "sticky client" problems and Hotspot 2.0 eases secure device onboarding.

6 Access Network Connectivity Requirements

6.1 Wireless Access Network Capabilities

6.1.1 Wireless Access Network Capabilities Intro

The wireless network is designed for automated and secure attachment of medical devices to the health care network. Essential capabilities of the network include:

- Automated network discovery and selection
- Mutual authentication of device and network with strong, commercially available security mechanisms
- Traffic priority and QoS for critical applications and devices
- Continuous service across APs as the medical device moves between locations
- Standard device interfaces for reliable, lower cost configuration

A number of IEEE and WFA specified technologies are leveraged to realize these capabilities. [WFA-Hotspot-2.0] specifies automated network discovery and selection per health care network operator policies. Hotspot 2.0 also specifies a standard device interface for secure SSID profiles, user credentials and operator network selection policy. [WFA-WPA2] (based upon [IEEE-802.11i-2004]) with EAP-TLS specifies mutual authentication of device and network using PKI. [WFA-WMM] (based upon [IEEE-802.11e-2005]) specifies application or device driven traffic priority. Continuous service across APs is specified by two technology sets. Fast BSS transitions (based upon [IEEE-802.11r-2008]) specifies the transfer of security contexts across APs with the same SSID. BSS Transition Management (based upon [IEEE-802.11k-2008]) specifies the over-the-air transfers of parameters that help devices select nearby APs to move to when present link conditions deteriorate. Wireless Network Management (based upon [IEEE-802.11v-2011]) specifies extended radio measurements and the exchange of network topology to help improve the performance of devices.

6.1.2 Air Interface Requirements

6.1.2.1 Air Interface Requirements Intro

This section addresses the air interface of The Center compliant Wi-Fi networks with a profile based upon [IEEE-802.11-2016] and related WFA specifications. A composite profile of [IEEE-802.11-2016] is specified below with a series of WFA specifications and certification programs. Please see IEEE and WFA documentation such as [IEEE-802.11-2016], [WFA-WMM] and [WFA-WPA2] Enterprise for further detailed definition of each requirement's category in the composite profile. It is desirable to leverage the global Wi-Fi ecosystem. Therefore, 802.11 and WFA requirements are defined by released WFA test procedures and profiles, except where noted.

6.1.2.2 STA Transmit Power Requirement

Clients that are STAs SHALL support a maximum transmit power (Tx) of 8 dBm or greater Equivalent Isotropically Radiated Power [EIRP].

6.1.2.3 STA PER Requirement

To ensure that medical devices will not consume excessive airtime with retransmissions, devices need to operate at a low PER under a typical data load at the cell edge. The Cell Edge Environment [CEE] is defined with a signal level of -63dBm, an SINR of 24dB, and an ambient channel utilization of ten percent. Clients that are STAs SHALL be capable of resolving traffic and associating to an AP at 24Mbps in the CEE. Clients that are STAs SHALL be capable of operating at or under an average PER of 2.5% over 1000 frames, representative of clinical function, in the CEE. The STA MAY use adaptive rate selection.

6.1.2.4 STA Certification Requirement

The client that is a STA SHALL demonstrate capability, to the normative strengths listed in the STA column of Table 1, by meeting all requirements of the certifications listed in the Referenced Certification column of Table 1.

Table 1: Air Interface Requirements and Certifications

Requirement from 802.11 Standard	Referenced Certification	Client (STA)
802.11n capabilities dual band	Wi-Fi CERTIFIED n	SHALL
802.11e (WMM) QoS	WMM	SHALL
802.11i: WPA2-Enterprise with EAP-TLS	WPA2 - Enterprise EAP-TLS	SHALL
802.11w: Protected Mgmt Frames (PMF)	WPA2-Enterprise with Protected Management Frames	SHALL
802.11h: Dynamic Frequency Selection (DFS)	FCC KDB 905462	SHALL (Client mode without radar detection)
At least 8 dBm EIRP	Referenced in FCC compliance test results documentation	SHALL

6.1.2.5 STA Roaming requirements

6.1.2.5.1 STA Roaming Requirement Intro

Roaming capability of the STA is a critical factor in ensuring a reliable connectivity experience. Aspects of STA design that prevent stickiness (i.e. staying connected to an AP at low signal levels and data rates) are fundamental to the connectivity experience. Additionally, required use of EAP-TLS authentication methods increases association time and volume of traffic. Therefore,

STA design needs to include methods to reduce this burden on the user and network if it stands to support the intended use case.

6.1.2.5.2 STA 802.11r Requirement

STA clients SHOULD support 802.11r (Fast BSS Transitions by the Over-the-Air (OTA) method) to reduce reassociation time as a compensatory measure for the large overhead of EAP-TLS associations mandated in Wi-Fi Access Security Requirements. It is expected that some stations will be able to tolerate longer reassociation times without any impact on clinical performance and may submit evidence to this effect in lieu of supporting 802.11r. The required 802.11r feature profile is fully described in [WFA-Agile-1.2].

6.1.2.5.3 STA Clients Roaming Option Requirement

STA Clients SHALL support all requirements in the Network Assisted Roaming Option OR all the requirements in the Configurable Device Roaming Option. STA clients MAY support both options to facilitate exchange of management information, accommodate graceful load balancing, and ensure a uniform, interoperable experience on the WLAN.

6.1.2.5.3.1 Network Assisted Roaming Option

Network Assisted Roaming STA clients SHALL support 802.11k (BSS Transition Management) and 802.11v (Exchange of Network Topology). 802.11k conformant STAs improve network information gathering and collectively improve roaming decisions with the aid of the network. 802.11v conformant STAs improve roaming decisions and enable network input to these decisions, such as load balancing an especially station-dense room. Required 802.11k and 802.11v feature profiles are fully described in the Agile Multiband specifications and test plan [WFA-Agile-1.2]. Cellular capability is not required to complete this profile, nor is EAP-TTLS-MSCHAPv2, though these features MAY be included and MAY be tested in the Agile Multiband program.

6.1.2.5.3.2 Configurable Device Roaming Option

This section contains requirements for Configurable Device Roaming. Goals of these requirements are to prevent sticky clients and eliminate slow roaming. A sticky client is one that does not roam when the signal strength of a candidate AP exceeds the signal strength of the serving AP by a specified dB level. Once the specified signal level is exceeded, the roam initiation delay time starts at the first transmitted frame from the STA on the serving AP and stops at the last transmitted frame from the STA on the serving AP.

To prevent client stickiness, a Configurable Device Roaming STA client SHALL start to roam (roaming initiation delay) within 30 seconds, or less time to support the intended application, when the sustained signal level of a candidate AP exceeds the serving AP signal level by 9dB. Note that if the STA client has a minimum signal level of -63dBm from the currently associated AP, with low interference, then a roam action is not required.

A slow roaming client does not roam within a desired timeframe. To eliminate slow roaming clients, a Configurable Device Roaming STA client SHALL complete a roam within 5 seconds. STA clients SHOULD support channel masking, to be configured for each HDO, to reduce off-channel scan time during roaming.

A roam is defined by identifying the last acknowledged encrypted frame sent by the STA client on the previous AP and identifying the last EAPOL frame or acknowledged reassociation response frame sent by the STA client on the new AP. The time delta between the aforementioned frames is known as the roam time, shown in Figure 3.

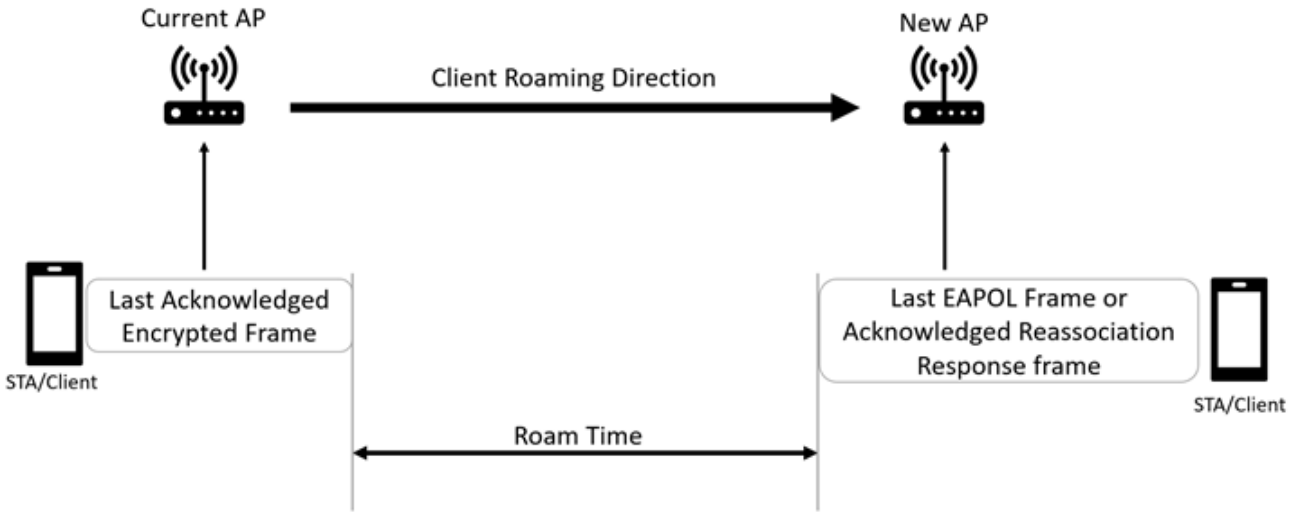

Figure 3 - Calculating STA/Client Roam Time

Figure 4 shows signal levels experienced by a client while roaming. As the STA moves from left to right, it needs to roam from the serving AP (left) to the candidate AP (right) within 5 seconds of detecting a 9dB delta. The signal value at the cell edge and the 9dB delta may vary based on the HDO network. The signal values at the STA will also vary based on the velocity of the STA.

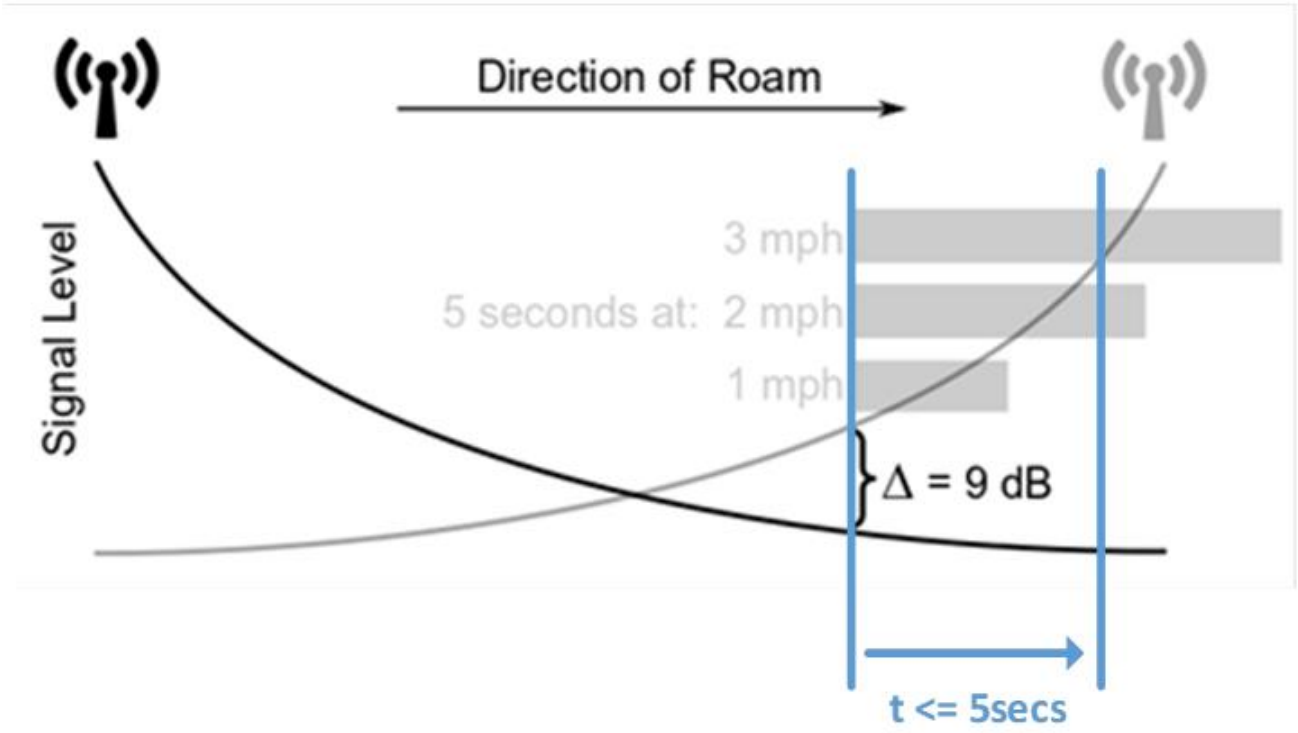

Figure 4 - Typical Roaming Profile

6.1.2.6 AP Roaming

It is important that APs support advanced roaming enhancements to enable better performance from STAs that support these features. APs need to support 802.11k (BSS Transition Management), 802.11r (Fast BSS Transitions by the Over-the-Air (OTA) method), and 802.11v (Exchange of Network Topology). The required 802.11k, 802.11r, and 802.11v feature profiles are fully described in [WFA-Agile-1.2].

6.1.2.7 WFA Hotspot 2.0 requirements

The [WFA-Hotspot-2.0] specification describes mandatory and optional Hotspot 2.0 requirements and capabilities. The WFA Passpoint certification program verifies these requirements. Table 2 lists the WFA certifications required by CMI. Please see the WFA Hotspot 2.0 specification for a complete definition of the requirements.

The client that is an STA SHALL demonstrate capability, to the normative strengths listed in the STA column of Table 2, by meeting all requirements of the certifications listed in the Referenced Certification column of Table 2.

Table 2: WFA Hotspot2.0 Requirements and Certifications

Requirements from IEEE and WFA Standards	Referenced Certification	Client (STA)
GAS and ANQP queries	Passpoint Release 2	SHALL
Interworking information element, including its Venue Info and Homogeneous Extended Service Set Identifier (HESSID)	Passpoint Release 2	SHALL
Roaming Consortium OI	Passpoint Release 2	SHALL
BSS Load Element	Passpoint Release 2	SHALL
IP Address type availability	Passpoint Release 2	SHALL
3GPP cellular network	Passpoint Release 2	MAY
Domain Name	Passpoint Release 2	SHALL
HS Query List	Passpoint Release 2	SHALL
WAN Metrics	Passpoint Release 2	SHALL
Connection Capability	Passpoint Release 2	SHALL
NAI Home Realm Query	Passpoint Release 2	SHALL
Proxy ARP	Passpoint Release 2	SHALL
Operating Class Indication	Passpoint Release 2	SHALL

Requirements for operator policy for network detection and selection per the parameters in Table 2 are given in the device provisioning section.

6.1.2.8 Wi-Fi Provisioning Interface

[Editor's note: Wi-Fi provisioning interface requirements may be specified in a future iteration of this specification]

6.2 Security

6.2.1 Architecture

6.2.1.1 Secure Communication Requirement

All management and clinical communications between Connected Components SHALL be secured. This is achieved by creating security associations at the Link Layer in accordance with this specification and at the Network Layer in accordance with [CMI-SP-F-PF].

6.2.1.2 Identity Elements Requirement

Identity elements (certificates and keys) SHALL be installed and managed in accordance with [CMI-SP-F-ID].

6.2.1.3 Access Network Security Architecture Summary

The access network security architecture controls access to the core hospital network using device authentication and authorization, securing the connection with encryption and message integrity. The access network security architecture is illustrated in Figure 5.

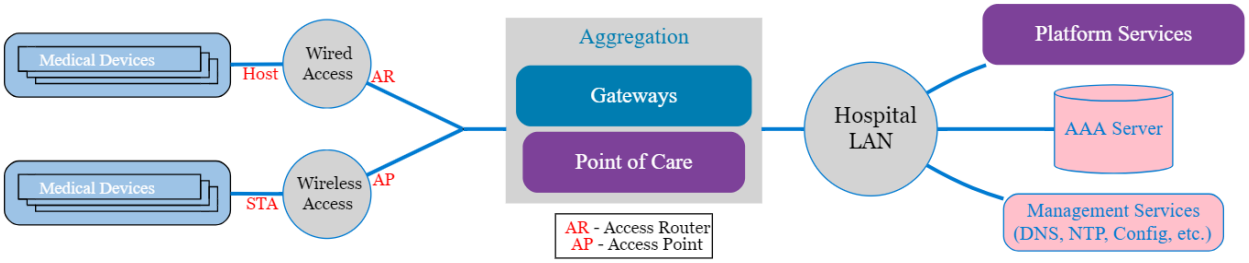

Figure 5 - Access Network Security Architecture

[IEEE-802.1X-2010] is used to mutually authenticate devices and exchange keys for secure access to the core hospital network (LAN). When a Medical Device first connects to the network it performs mutual authentication with the AAA server using EAP-TLS and certificate credentials issued from The Center's PKI. The Access Router and Hotspot 2.0 Wi-Fi AP forward this authentication messaging between the Medical Device and AAA server.

After the AAA server authenticates the Medical Device it must check that the Medical Device is authorized to connect to the core network using the Medical Device's identifier. Medical Device authorization is out of scope for this version of the document.

If mutual authentication and authorization are successful, keys are exchanged to secure the access network connection. The AAA Server sends a session key derived from authentication messaging parameters to the Access Router or Wi-Fi AP. The Medical Device derives the same session key from authentication messaging parameters. The Access Router or Wi-Fi AP then allows traffic from the Medical Device, encrypted with the session key, access to the hospital core network after it has been decrypted. Once network access has been granted to the Medical Device, a security association is established with the Management Entity for application services (see [CMI-SP-F-PF]).

The RADIUS connection between the AAA server and Access Router or Hotspot 2.0 Wi-Fi AP needs to be secure to protect the session keys. Furthermore, all other core network management connections should also be protected. Pre-shared key credentials with the IKEv2/IPsec protocol are commonly used to secure these types of connections. Specification of how these connections are secured is out of scope of this document as compensating controls and left to hospital IT and security staff.

To support secure access as specified here, Access Routers and APs need to support requisite features. Access Routers need to support [IEEE-802.1X-2010] and [IEEE-802.1AE-2006] requirements. Wi-Fi APs need to be Hotspot 2.0 R2 compliant. However, these elements are out of scope.

6.2.2 Wi-Fi Access Security Requirements

6.2.2.1 Wi-Fi Access Security Requirements Intro

Wi-Fi network access security uses Hotspot 2.0 security features, which are based on 802.1X, and the certificate PKI defined in The Center's Certificate Policy [CMI-SP-F-CP] to establish an authenticated, secure connection. The Medical Device and AAA Server exchange certificates for mutual authentication using the EAP-TLS protocol. After successful authentication keys are exchanged to encrypt the wireless link using WPA2.

6.2.2.2 Client STA Requirement

The client that is a STA SHALL demonstrate capability, to the normative strengths listed in the STA column of Table 3.

Table 3 Hotspot 2.0 Security Capability List

Requirement	WFA Hotspot 2.0 Reference	Client (STA)
EAP-TLS authentication messaging	Mandatory	SHALL
WPA2-Enterprise	Mandatory	SHALL
AAA Server cert validation, no bypass	Mandatory	SHALL
Client/device certificate credential support	Mandatory	SHALL
Remote client/device certificate enrollment/update	Mandatory	Allowed only if controlled by Medical Device manufacturer

6.2.3 Wired Access Security Requirements

6.2.3.1 Wired Access Security Requirements Intro

Wired network access security uses 802.1X security features and the certificate PKI defined in The Center's Certificate Policy [CMI-SP-F-CP] to establish an authenticated, secure connection. The Connected Component and AAA Server exchange certificates for mutual authentication using the EAP-TLS protocol. After successful authentication, the AAA server and Access Router exchange keys to encrypt the wired link between the Access Router and Connected Component using MACsec.

When setting up the hospital network, all wired ports must be secured using a compliant Access Router with 802.1X credentials for core medical network (VLAN) access. Ports must be placed into a guest (DMZ) network (VLAN) or disabled if 802.1X credential requirements are not met.

6.2.3.2 Wired Client Authentication Requirement

The IP enabled, wired client SHALL support [IEEE-802.1X-2010] and [IEEE-802.1AE-2006] supplicant requirements. The client SHALL support EAP-TLS [IETF-RFC5246] as the method for certificate based mutual authentication.

6.2.4 Client Access Security Requirements

6.2.4.1 Client Secure Transport Using TLS Requirement

The client SHALL conform to TLS Interface B requirements [CMI-SP-F-PF] (Annex B) for communicating with AAA infrastructure during the 802.1X EAP-TLS authentication and authorization process.

6.2.5 Checking for Certificate Revocation

6.2.5.1 HDO Network Equipment Secure Transport Using TLS Requirement

HDO network equipment responsible for onboarding clients (e.g. AP, WAC, AAA server) will conform to TLS Interface A requirements [CMI-SP-F-PF] (Annex B) for communicating with CMI compliant clients during the 802.1X EAP-TLS authentication and authorization process.

6.2.6 AAA Server Requirements

AAA servers will enable authentication and authorization. To support the requirements of these specifications, AAA servers must support the following requirements. While AAA servers are out of scope, these requirements are described for clarity.

- The AAA Server needs to be [WFA-Hotspot-2.0] compliant.
- The AAA Server needs to meet [FIPS-140-2] security requirements for all instances of private and public key permanent storage. This includes compliance to level 1 security protections which requires an enclosure to help prevent unauthorized access.
- The AAA Server needs to support [IEEE-802.1X-2010] Authentication Server requirements.

7 Acknowledgements

The Center and its member companies would like to extend a heartfelt thanks to all those who participated in the development of this document.

Bernie McKibben authored this original version of this document with input from **Mitchell A. Ross, Bowen Shaner** and **David Fann** (Trusted Wireless Health related Requirements); and **Stuart Hoggan** and **Steve Georinger** (Security requirements). **Bowen Shaner** and **Sumanth Channabasappa** worked collaboratively to revise this D02 version. Bowen Shaner is the CMI Lead for this document.

This work was conducted within the Center's Architecture & Requirements, and Connectivity working groups and reviewed by the Security working group, whose members have including the following part-time and full-time participants during the creation of this version of the document:

Working Group Participants	Company Affiliation
Aishwarya Muralidharan	vTitan
Alex Poiry	Cerner
Ali Nakoulima	Cerner
Andrew Meshkov	86Borders
Brian Long	Masimo
Brian Scriber	CableLabs
Bruce Friedman	GE Healthcare
Corey Spears	Infor
Darshak Thakore	CableLabs
David Hatfield	Becton Dickenson
David Niewolny	RTI
Eldon Metz	Innovision Medical
George Cragg	Draeger
Guy Johnson	Zoll
Ian Sherlock	Texas Instruments
James Surine	Smiths-Medical

Working Group Participants	Company Affiliation
Jason Mortensen	Bernoulli Health
Jay White	Laird
Jay White	Laird
Jeffrey Brown	GE
JF Lancelot	Airstrip
John Barr	CableLabs
John Hinke	Innovision Medical
John Williams	FortyAU
Kai Hassing	Philips
Ken Fuchs	Draeger
Logan Buchanan	FortyAU
M Prasannahvenkat	vTitan
Massimo Pala PhD	CablelLabs
Mike Krajnak	GE
Milan Buncick	Aegis
Neil Puthuff	RTI
Neil Seidl	GE
Ponlakshmi G	vTitan
Scott Eaton	Mindray
Stefan Karl	Philips
Steven Goeringer	CableLabs
Travis West	Bridge Connector

- Sumanth Channabasappa (Chief Architect),, Steve Goeringer (Chief Security Architect), Chris Riha (Working Groups Lead), Paul Schluter, Bowen Shaner, Jacob Chadwell, David Fann, Spencer Crosswy, Dr. Richard Tayrien, Trevor Pavey; and, Ed Miller (CTO) - The Center