CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Specification
Access Network Connectivity

CMI-SP-F-ANC-D01-20190311

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.

Document Status Sheet

Document Control Number:	CMI-SP-F-ANC-D01-20190311			
Document Title:	Access Network Connectivity			
Revision History:	D01			
Date:	March 11, 2019			
Status:	~~Work in Progress~~	**Draft**	~~Issued~~	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~The Center/Member~~	~~The Center/ Member/ NDA Vendor~~	**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 in specification format 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.

Contents

1 Scope 5
1.1 Introduction and Purpose 5
1.2 Requirements 5
2 References 6
2.1 Normative References 6
2.2 Reference Acquisition 8
3 Terms and Definitions 9
4 Abbreviations and acronyms 9
5 WIRELESS ACCESS NETWORK OVERVIEW 11
5.1 End-to-End Architecture 11
5.1.1 Hotspot 2.0 applied to Wi-Fi networks 11
5.1.2 Backwards compatibility with WPA2 Enterprise 12
5.2 Access Network Connectivity Flow 12
5.3 Access Network Design – Trusted Wireless Health 13
6 Access Network Connectivity Requirements 13
6.1 Wireless Access Network Capabilities 13
6.1.1 Air Interface Requirements 14
6.2 Security 19
6.2.1 Architecture 19
6.2.2 Wi-Fi Access Security Requirements 21
6.2.3 Wired Access Security Requirements 22
6.2.4 Checking for Certificate Revocation 23
6.2.5 AAA Server Requirements 23
Appendix I. Acknowledgements 26

Figures

Figure 1-Wi-Fi Access Network Architecture Diagram 11
Figure 2-High Level Functional Flow of Network Access 13
Figure 3 - Calculating STA/Client Roam Time 17
Figure 4 - Typical Roaming Profile. 17
Figure 5-Access Network Security Architecture 20

Tables

Table 1: Air Interface Requirements and Certifications 15
Table 2: WFA Hotspot2.0 Requirements and Certifications 18
Table 3 Hotspot 2.0 Security Capability List 21

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 two fold: 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-DOC-TD]	"Terms and Definitions", Center for Medical Interoperability, Mar. 2019 https://medicalinteroperability.org/specifications/D01/CMI-DOC-TD-D01-20190311.pdf
[CMI-SP-F-ID]	"Identity Specification", Center for Medical Interoperability, Mar. 2019 https://medicalinteroperability.org/specifications/D01/CMI-SP-F-ID-D01-20190311.pdf
[IEEE-802.11-2016]	IEEE 802.11: 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, 2016. https://standards.ieee.org/standard/802_11-2016.html
[IEEE-802.11d-2001]	IEEE 802.11d: Amendment 3: Specification for operation in additional regulatory domains, 2001. https://standards.ieee.org/standard/802_11d-2001.html

[IEEE-802.11e-2005] IEEE 802.11e: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005.

https://standards.ieee.org/standard/802_11e-2005.html

[IEEE-802.11g-2003] IEEE 802.11g: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 2003

https://standards.ieee.org/standard/802_11g-2003.html.

[IEEE-802.11i-2004] IEEE 802.11i: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

https://standards.ieee.org/standard/802_11i-2004.html

[IEEE-802.11k-2008] IEEE 802.11k: Amendment 1: Radio Resource Management for WLANs, 2008

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

[IEEE-802.11n-2009] IEEE 802.11n: Enhancement for higher throughput, 2009.

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

[IEEE-802.11r-2008] IEEE 802.11r: Amendment for fast BSS Transitions, 2008.

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

[IEEE-802.11v-2011] IEEE 802.11v: Wireless Network Management, 2011.

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

[IEEE-802.1X-2010] IEEE 802.1X: Port-Based Network Access Control (PNAC), Feb. 2010

https://standards.ieee.org/content/ieee-standards/en/standard/802_1X-2010.html

[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-WPA2] Wi-Fi Alliance: Wi-Fi Protected Access (WPA) Enhanced Security Implementation Based on IEEE P802.11i standard, Version 3.1, August, 2004.

https://www.wi-fi.org/discover-wi-fi/security

[WFA-WMM] Wi-Fi Alliance: Wi-Fi Multi-Media QoS based on 802.11e, Version 1.1, 2012..

https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm-programs

[ITU-T-X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-201610-I!!PDF-E&type=items

[IETF-RFC5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

https://tools.ietf.org/html/rfc5280

[IETF-RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013.

https://tools.ietf.org/html/rfc6960

[WFA-Agile-1.1] Wi-Fi Alliance: Agile Multiband Technical Specification V1.1.1, 2017

https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_Agile_Multiband_Specification_v1.1.pdf/34975

2.2 Reference Acquisition

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

Institute of Electrical and Electronics Engineers (IEEE), 3 Park Avenue, 17th Floor, New York, NY 10016-5997; http://www.ieee.org/

Wi-Fi Alliance, 10900-B Stonelake Boulevard, Suite 126, Austin, Texas 78759, http://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 in [CMI-DOC-TD], and the following:

Hotspot 2.0	Capabilities defined by the WFA that bring a cellular-like network roaming to Wi-Fi
Trusted Wireless Health	The Center's guidelines to provide security, reliability and performance needed for health care Wi-Fi networks

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
CHAP	Challenge Handshake Authentication Protocol
CRL	Certificate Revocation List
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards
GAS	Generic Advertisement Service
HDO	Healthcare Delivery Organization
HS	Hotspot
IKE	Internet Key Exchange

IPsec	Internet Protocol Security
NAI	Network Acces Identifier
OCSP	Online Certificate Status Protocol
PER	Packet Error Rate
PKI	Public Key Infrastructure
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SSID	Service Set Identifier
STA	Station
UNII	Unlicensed National Information Infrastructure
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 functional end-to-end architecture for medical devices that connect to Wi-Fi networks. Functional elements are identified and described.

A conceptual message flow is shown in Figure 1 that illustrates how medical devices discover, mutually authenticate and then attach to the health care provider's wireless access network with leveraging Hotspot 2.0.

Section 6 specifies Wi-Fi access network connectivity for medical devices that connect to a health system's access network. It specifies the use of Hotspot 2.0 for connecting to access networks. It also includes the device configuration requirements to support The Center's Trusted Wireless Health requirements.

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.

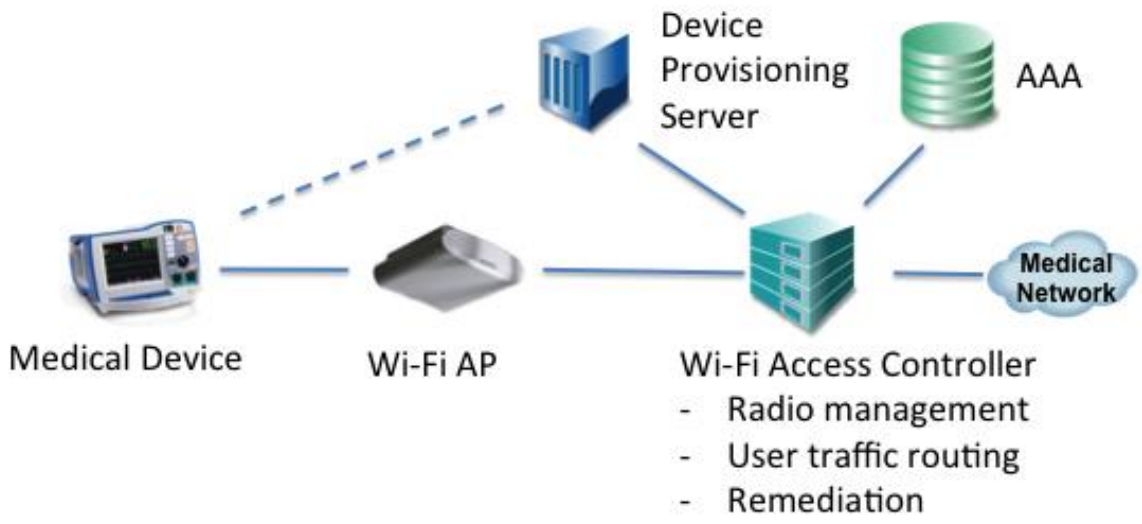

Figure 1-Wi-Fi Access Network Architecture Diagram

The medical device connects to the Wi-Fi AP over The Center specified air interface. Key capabilities on the AP air interface include 802.11n, WMM for QoS, WPA2 enterprise for security, fast transitions across AP, and HS2.0 for automated network discovery and selection. The AP is controlled by the Wi-Fi Access Controller (WAC). The Controller provides a number of functions including radio resource management, user traffic routing and Hotspot 2.0 specified user access remediation. The Device Provisioning Server configures the Wi-Fi air interface on medical devices. 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 medical devices to the health care provider's Wi-Fi network. It can also be used to account for medical device usage of network resources. The AAA may hold the medical device subscriptions to the health care wireless network, or interface to an external database that holds the subscriptions.

This specification focuses on requirements to the medical device and the Wi-Fi AP. 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 is mandated for The Center specified Wi-Fi AP air interface. 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 the pace that meets the needs of the health organization. A single SSID can simultaneously support both Hotspot 2.0 devices and legacy devices with WPA2-Enterprise.

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.

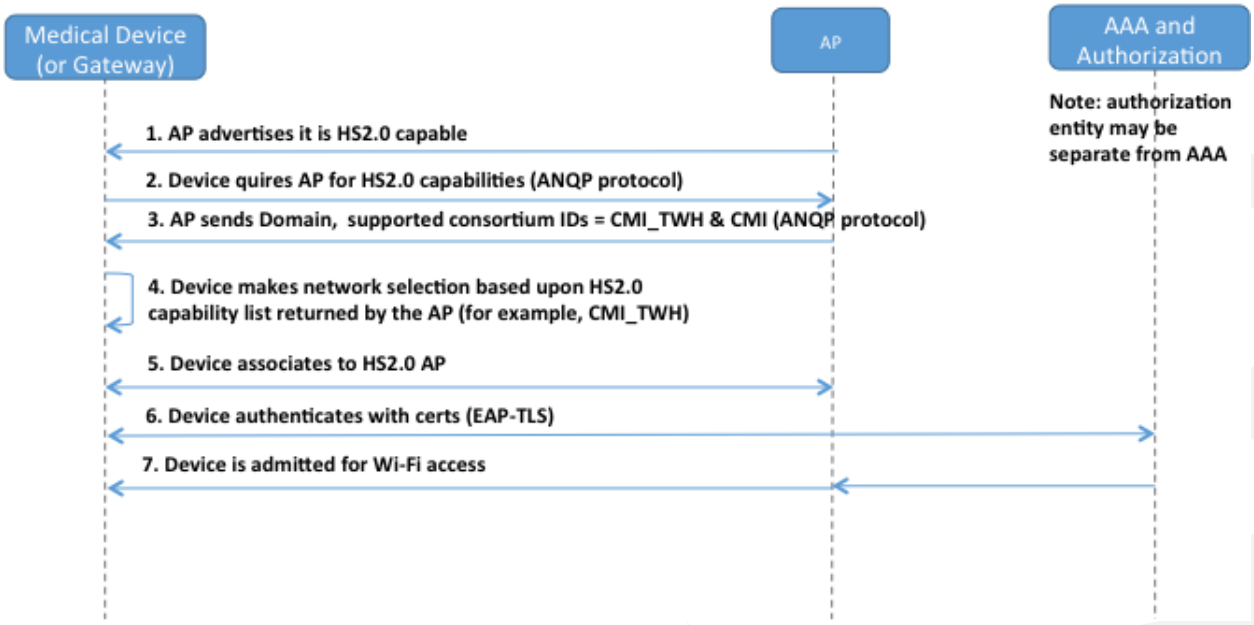

Figure 2-High Level Functional Flow of Network Access

As shown in Figure 2, the Hotspot 2.0 AP advertises that it is Hotspot 2.0 capable per information elements as specified in 802.11. 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 third message of the flow, the AP indicates it roaming capability to support two consortium IDs, the CMI_TWH consortium and the CMI consortium. CMI indicates that the network is ready to receive CMI compliant devices. CMI_TWH indicates that the network supports TWH requirements. The device is configured to select the AP for association based upon the preferred consortium ID of 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 authenticates the certificate received from the device, and thereby completes the mutual authentication process. The AAA admits the device onto the secured Wi-Fi air interface as authorized by the medical network. The authorization process is not shown in the diagram. Once the AP receives admission authorization and over the air cryptographic keys 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) networks are tuned to ensure consistent, strong signals for many overlapping layers of traffic. TWH network design begins as 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 by limiting AP transmit power to 8 dBm and cell edge 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. Many elements of this specification are intended to optimize device operation in TWH environments, such as IEEE wireless roaming standards that address "sticky client" problems and Hotspot 2.0 that eases secure device onboarding.

6 Access Network Connectivity Requirements

6.1 Wireless Access Network Capabilities

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 the critical applications and devices

- Continuous service across APs as the medical device moves between locations
- Standardized device interfaces for reliable, lower cost configurations

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 Enterprise (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.

6.1.1 Air Interface Requirements

This section addresses the air interface of The Center compliant Wi-Fi network 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 Wi-Fi Alliance test procedures and profiles, except where noted as altered or excluded.

Medical clients that are STAs SHALL support a minimum transmit power (Tx) of 8 dBm Equivalent Isotropically Radiated Power [EIRP].

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. In order to support reasonable test times, the device clients SHALL generate a minimum of 1000 messages/packets representative of typical communication patterns within 30 minutes. In some cases, for low bandwidth devices such as infusion devices and vital signs monitors, this data may need to be generated via special test SW or tooling.. Iperf is an example tool that can be used to create a data load.

The medical 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 certification tests listed in the Referenced Certification column of Table 1.

Table 1: Air Interface Requirements and Certifications

Requirement from 802.11 Standard	**Referenced Certification**	**Medical 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

6.1.1.1 STA Roaming requirements

Roaming capability of the STA is a critical factor in ensuring a reliable connectivity experience. Aspects of the STA design that prevent stickiness (i.e. staying connected to an AP at low signal levels and data rates) are fundemental 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.

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 Section 6.2.2. 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 the Wi-Fi Agile Multiband technical specification [Agile] and test plan.

Station clients SHALL support all requirements in the Network Assisted Roaming Option (Section 6.1.1.1.1) OR all the requirements in the Configurable Device Roaming Option (Section 6.1.1.1.2).

Station clients MAY support both options to facilitate exchange of management information, accommodate graceful load balancing, and ensure a uniform, interoperable experience on the WLAN.

6.1.1.1.1 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. 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.

6.1.1.1.2 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 a desired signal strength or RSSI of a candidate AP exceeds the serving AP signal level by a specified dB level. Once the specified signal level of 9db is exceeded, the roaming 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 a sustained signal level of a candidate AP exceeds the serving AP signal level by 9 dB.

A slow roaming client that 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.

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 packets is also known as the “roam time” as shown in Figure 3.

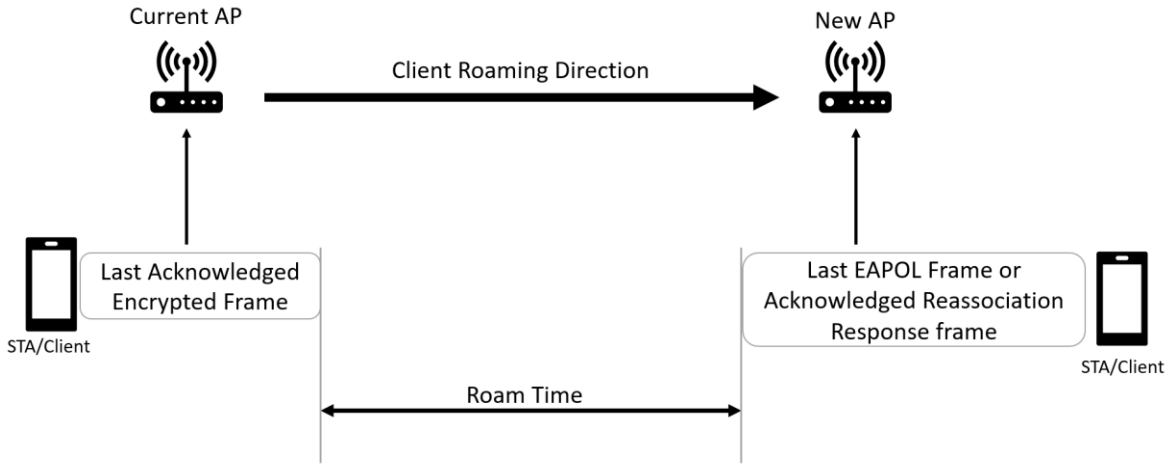

Figure 3 - Calculating STA/Client Roam Time

Device clients SHOULD support channel masking, to be configured for each HDO, to reduce off-channel scan time during roaming.

A device client's decision making process for AP roam candidates should not be considered part of the "roam time"

Note that if the STA client is within a minimum signal level of -63dbm or better from a currently associated AP with low interference, then a roam action is not required. To test the configurable device roaming requirement, AP signal levels at the STA will vary according to a profile representative of a hospital environment as shown in Figure 4.

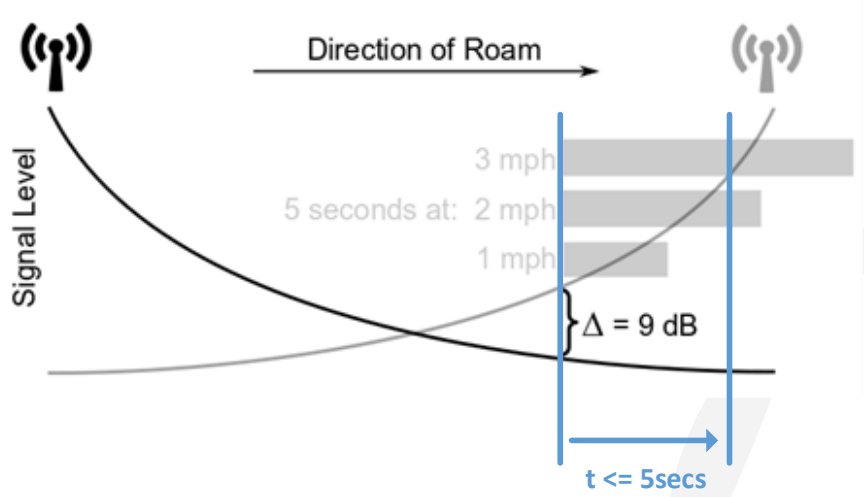

Figure 4 - Typical Roaming Profile.

As a 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 9 dB 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.

6.1.1.2 AP Roaming

It is important that the 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 the Wi-Fi Agile Multiband technical specification.

6.1.1.3 WFA Hotspot 2.0 requirements

This section mandates the WFA Hotspot 2.0. The WFA Hotspot 2.0 specification describes mandatory and optional Hotspot 2.0 requirements and capabilities. The WFA Passpoint certification program verifies these requirements. The following 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 medical 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 certification tests 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	Medical 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 ID	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

Requirements from IEEE and WFA Standards	Referenced Certification	Medical Client (STA)
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.

6.1.1.4 Wi-Fi Provisioning Interface

[Editor's note: the Wi-Fi provisioning interface requirements will be specified in the next iteration of the specification.]

6.2 Security

6.2.1 Architecture

All management and clinical communications to Platforms, Gateways, and Medical Devices (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 [IHE PCD HL7]. Identity elements (certificates and keys) SHALL be installed and managed in accordance with [CMI-SP-F-ID].

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

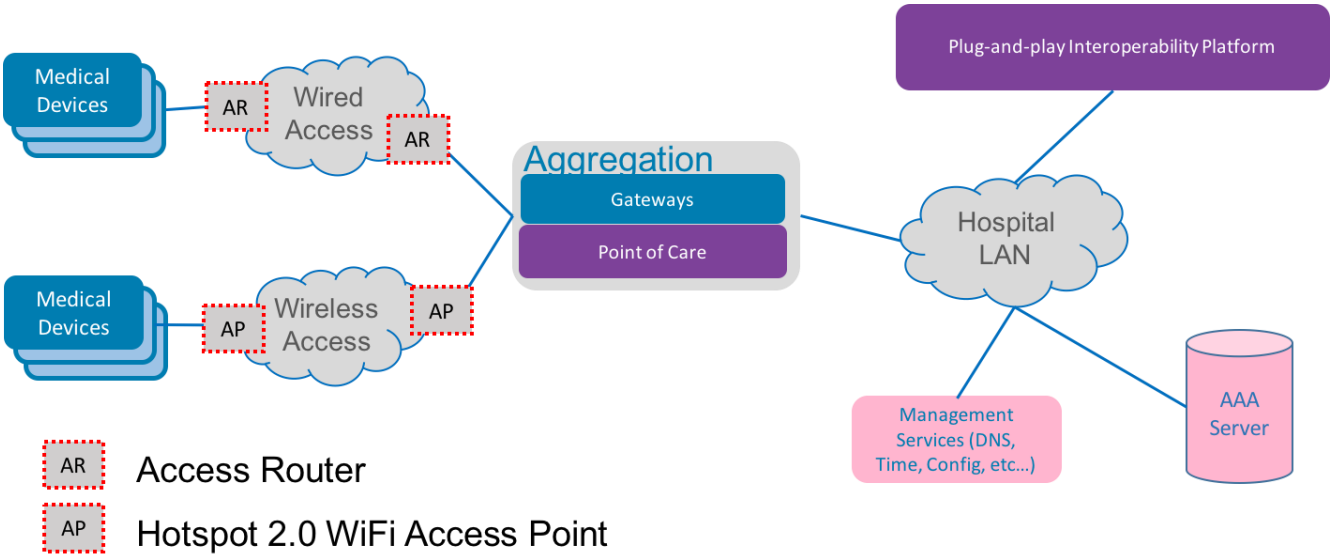

Figure 5-Access Network Security Architecture

802.1x 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 to access the hospital core network after it has been decrypted. Once network access has been granted to the Medical Device a security association is then established with the Platform for application services (see [IHE PCD HL7]).

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. Preshared key credentials with the IKEv2/ISPsec 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 802.1x-2010 and 802.1ae (MACsec) Authenticator

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

Wi-Fi network access security uses Hotspot/Passpoint 2.0 security features, which are based on 802.1x, and the certificate PKI defined in The Center's Certificate Policy 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.

The medical 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**	**Medical 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

Connected Component Requirements:

1. The Medical Device SHALL be Hotspot 2.0 R2 compliant.
2. The Connected Component ECC or RSA certificate, private key, and issuing CA certificate as defined in [CMI-SP-F-ID] SHALL be securely installed in the Connected Component. Any removable modules supported by the Medical Device (e.g., a removable Wi-Fi module) SHALL NOT contain the Medical Device certificate, private key, and issuing CA certificate.
3. The root CA certificate defined in The Center's Certificate Policy and authorized by CMI SHALL be installed in the Medical Device as a trust anchor for validating received certificates.
4. During EAP-TLS authentication messaging the Medical Device SHALL include the issuing CA certificate with its own certificate in the EAP-TLS Certificate message.

5. The Medical Device SHALL validate certificates received from the AAA Server using Basic Path Validation procedures defined in the X.509 PKI certificate standard [RFC 5280] and verify that the host portion of the AAA Server URL matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the server certificate. It SHALL also check that the certificates are not revoked. If the Medical Device cannot validate the received certificates it SHALL reject AAA Server authentication, log an error, and periodically retry the connection

6. When a Conencted Component validates received certificates it checks their revocation status using Online Certificate Status Protocol, OCSP, [IETF-RFC6960].

7. The STA SHALL store the Certificate private key in a manner that deters unauthorized disclosure and modification. The STA SHALL meet security requirements for all instances of private and public permanent key storage according to [CMI-SP-F-ID].

6.2.3 Wired Access Security Requirements

Wired network access security uses 802.1x security features and the certificate PKI defined in The Center's Certificate Policy 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.

Connected Component Requirements:

8. The Medical Device SHALL support 802.1x-2010 and 802.1ae (MACsec) Supplicant requirements. The Medical Device SHALL support EAP-TLS as the method for certificate based mutual authentication.

9. The Connected Component ECC or RSA certificate, private key, and issuing CA certificate as defined in [Identity] SHALL be securely installed in the Connected Component. Any removable modules supported by the Medical Device (e.g., a removable Wi-Fi module) SHALL NOT contain the Medical Device certificate, private key, and issuing CA certificate.

10. The root CA certificate defined in The Center's Certificate Policy and authorized by CMI SHALL be installed in the Medical Device as a trust anchor for validating received certificates.

11. During EAP-TLS authentication messaging the Medical Device SHALL include the issuing CA certificate with its own certificate in the EAP-TLS Certificate message.

12. The Medical Device SHALL validate certificates received from the AAA Server using Basic Path Validation procedures defined in the X.509 PKI certificate standard [IETF-RFC5280] and verify that the host portion of the AAA Server URL matches the Common Name attribute of the Subject

field or any domain names in the Subject Alternative Name extension in the server certificate. It SHALL also check that the certificates are not revoked. If the Medical Device cannot validate the received certificates it SHALL reject AAA Server authentication, log an error, and periodically retry the connection

13. The STA SHALL store the Certificate private key in a manner that deters unauthorized disclosure and modification. The STA SHALL meet security requirements for all instances of private and public permanent key storage according to [CMI-SP-F-ID].

6.2.4 Checking for Certificate Revocation

Clients, access points, and routers SHALL check the revocation status every certificate and every certificate in the certificate's chain up to (but excluding) the Root CA. Two different revocation status checking mechanisms SHALL be supported. The first one (and preferred) is OCSP while the second (backup mechanism) is CRLs. In particular, during certificate validation, the Platform first uses OCSP to check the revocation status and then MAY use a CRL if the OCSP server access or fresh OCSP responses are not available. The following revocation requirements apply to the Connected Component:

14. The latest version of the CRLs signed by The Center's root CA and Connected Component CA SHALL be installed on the component during setup. The component SHALL attempt to update these CRLs before they expire using the distribution server URL in the CRL header.

15. When performing certificate validation the component SHALL first check revocation status using OCSP. In case the OCSP responses are not provided via the TLS handshake or they are not available in the local cache, the component MAY retrieve the OCSP server URLs from the Connected Component certificate and the Connected Component CA certificate. If the OCSP URL is not available (e.g., not present in the certificate to be validated or not locally configured), the component SHALL use the CRL. Also in this case, the CRL SHOULD be retrieved from the URL specified in the certificates that are being validated (i.e., in the cRLDistributionPoints extension) and MAY be retrieved from a local cache if available. OCSP Responses and CRLs SHALL first be validated for authenticity and freshness before they can be used to check the revocation status of a certificate.

16. If a certificate has been revoked, the component SHALL reject Connected Component authentication, log an error, and close the connection.

6.2.5 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.

17. The AAA Server needs to be Hotspot 2.0 compliant.

18. The AAA Server needs to be configured to use EAP-TLS for certificate based mutual authentication.

19. The AAA Server certificate, private key, and issuing CA certificate as defined in The Center's Certificate Policy needs to be securely installed in the AAA Server by the hospital IT administrator. The AAA Server needs to have both ECC and RSA certificates installed.

20. The root CA certificate defined in The Center's Certificate Policy and authorized by CMI needs to be installed in the AAA Server as a trust anchor for validating received certificates.

21. During EAP-TLS authentication messaging the AAA Server needs to include the issuing CA certificate with its own certificate in the EAP-TLS Certificate message. The AAA Server needs to select either its ECC or RSA certificate depending upon what type of Medical Device certificates (ECC or RSA) it receives.

22. The AAA Server needs to validate certificates received from the Medical Device using Basic Path Validation procedures defined in the X.509 PKI certificate standard [RFC 5280] and verify that the identifier value of the Common Name attribute in the Subject field is authorized. It needs to also check that the certificates are not revoked. The AAA Server needs to support validating ECC and RSA Medical Device certificates as defined in The Center's Certificate Policy. If the AAA Server cannot validate the received certificates it needs to reject Medical Device authentication, log an error and close the connection and not distribute a Master Session Key (MSK) to the Wi-Fi AP or Access Router.

23. When a AAA Server validates received certificates it checks their revocation status. Two revocation methods are supported: OCSP and CRL. First OCSP is used to check the revocation status and then the CRL is used if the OCSP server access is not available. The following revocation requirements apply to the AAA Server:

    - The latest version of the CRLs signed by The Center's root CA and Medical Device CA needs to be installed on the AAA Server during setup. The AAA Server needs to attempt to update these CRLs before they expire using the distribution server URL in the CRL header.

    - When performing certificate validation the AAA Server needs to first check revocation status using OCSP and the OCSP server URLs provided in the extensions of the Medical Device certificate and the Medical Device CA certificate. If an OCSP server is not available the AAA Server needs to use the CRL.

    - If a certificate has been revoked, the AAA Server needs to reject Medical Device authentication, log an error, and close the connection.

24. The AAA Server needs to support TLS Stapling for providing OCSP revocation status about its certificates to the Medical Device. The AAA Server forwards OCSP requests to the CA OCSP server URL embedded its server certificate and forwards OCSP responses to the Medical Device via the initial TLS message exchange.

25. 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.

26. The AAA Server nees to support 802.1x-2010 Authentication Server requirements.
27. The AAA Server needs to support the same certificate related requirements as defined for Wi-Fi access (see Section 6.2.2).
28. The AAA Server needs to support the same key and certificate security storage requirements as for Wi-Fi access (see Section 6.2.2).

Appendix I. 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 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).

Special thanks to those who were directly involved via a variety of discussions, reviews and input: **Phil Raymond**, **Ken Fuchs, Matt Pekarske**and **Jay White**.

This effort was conducted within The Center's Connectivity Working Group, whose members have included the following part-time and full-time participants during the time period that we discussed this version of the document:

WG Participant	**Company Affiliation**
Bill Pelletier	GE
Bruce Friedman	GE
Dr. Jorg-Uwe Meyer	MT2IT
George Cragg	Draeger
James Surine	Smiths Medical
Jay White	Laird
John Zaleski	Bernoulli Health
John Williams	FortyAU
Ken Fuchs	Draeger
Logan Buchanan	FortyAU
Matt Pekarske	GE
Dr. Max Pala	CableLabs
Mike Krajnak	GE
Phil Raymond	Philips
Scott Coleman	Welch Allyn
Stuart Hoggan	CableLabs

- *Bernie McKibben (Primary Author, Connectivity Working Group Co-Lead), Sumanth Channabasappa (Connectivity Working Group Co-Lead), Steve Goeringer (Security Working Group Lead), Mitchell A. Ross, Bowen Shaner, David Fann, Trevor Pavey; and Ed Miller (CTO), The Center*