CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Specification Provisioning Flows

CMI-SP-F-PF-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-PF
Document Title:	Provisioning Flows
Revision History:	D02 IPR Review
Date:	03/15/2019
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 document addresses foundational requirements for clients in the areas of provisioning, operational resiliency, and management. This is a normative document and is intended for designers and architects of clients, and for technical operations personnel from the member community.

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-ANC] Access Network Connectivity

https://medicalinteroperability.org/specifications

[CMI-SP-F-ASUM] Automated Secure Update and Management Framework

https://medicalinteroperability.org/specifications

[CMI-SP-F-ID] Identity

https://medicalinteroperability.org/specifications

[FIPS-180-4] Secure Hash Standard (SHS), FIPS 180-4, August, 2015

https://csrc.nist.gov/publications/detail/fips/180/4/final

[FIPS-186-4] Digital Signature Standard (DSS), FIPS 186-4, July, 2013

https://csrc.nist.gov/publications/detail/fips/186/4/final

[IETF-RFC2131] Dynamic Host Configuration Protocol

https://tools.ietf.org/html/rfc2131

[IETF-RFC3315] Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

https://tools.ietf.org/html/rfc3315

[IETF-RFC3646] DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

https://tools.ietf.org/html/rfc3646

[IETF-RFC4704] The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option

https://tools.ietf.org/html/rfc4704

[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-RFC5288] AES Galois Counter Mode (GCM) Cipher Suites for TLS

https://tools.ietf.org/html/rfc5288

[IETF-RFC5289] TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), August 2008

https://tools.ietf.org/html/rfc5289

[IETF-RFC5908] Network Time Protocol (NTP) Server Option for DHCPv6

https://tools.ietf.org/html/rfc5908

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

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

[IETF-RFC6961] "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", IETF RFC, June 2013

https://tools.ietf.org/html/rfc6961

[IETF-RFC8422] Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier

https://tools.ietf.org/html/rfc8422

2.2 Informative References

[CMI-DOC-TD] Terms and Definitions

https://medicalinteroperability.org/specifications

[CMI-SP-CDI-IHE-PCD-SSE] Clinical Data Interoperability Based on IHE PCD – Semantics, Syntax, and Encoding

https://medicalinteroperability.org/specifications

[CMI-SP-F-CP] Certificate Policy

https://medicalinteroperability.org/specifications

2.3 Reference Acquisition

- Center for Medical Interoperability (The Center), 8 City Boulevard, Suite 203 | Nashville, TN 37209, USA; Phone +1-615-257-6410; https://medicalinteroperability.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

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:

AES	Advanced Encryption Standard
ANC	Access Network Connectivity
ASUM	Automated Secure Update Mechanism
CA	Certificate Authority
CDI	Clinical Data Interoperability
CDT	Clinical Data Transmission
CME	Client Management Entity
CMI	Center for Medical Interoperability
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name Service
ECC	Elliptic-Curve Cryptography
ECDHE	Elliptic-Curve Diffie-Hellman Ephemeral

ECDSA	Elliptic-Curve Digital Signature Algorithm
EHR	Electronic Health Record
FQDN	Fully Qualified Domain Name
HL7	Health Level Seven International
IHE PCD	Integrating the Healthcare Enterprise Patient Care Device
IP	Internet Protocol
MCCP	Minimum Connected Component Profile
MGMT	Management (see CME)
MLLP	Minimum Lower Layer Protocol
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PF	Provisioning Flow
PKI	Public Key Infrastructure
RSA	Rivest–Shamir–Adleman Cryptography
SHA	Secure Hash Algorithm
SSID	Service Set Identifier
TLS	Transport Layer Security
URL	Uniform Resource Locator
WG	Working Group

5 Overview

This document presents requirements related to three areas: provisioning flow, resiliency, and management. The scope is primarily the client. The provisioning flow specifies requirements for clients to connect to access networks and IP networks; acquire basic configuration parameters; and initiate clinical data communications. Resiliency ensures that the clients can identify and automatically recover from error scenarios. Client management functionality is outlined to enable technical operations personnel to monitor and address both minor and major issues related to client interactions. This document references other specifications that expand on specific areas, such as Access Network Connectivity [CMI-SP-F-ANC] and Automated Secure Update Mechanism (ASUM) [CMI-SP-F-ASUM].

6 Provisioning

6.1 Provisioning Requirements Intro

A client provisioning flow is the series of non-clinical communications undertaken by the client prior to clinical data communications. These include access network connectivity, IP network connectivity, retrieval of basic configuration, service discovery, requesting authorization, initiating secure software update if required, and initiating clinical data communications. These steps, and their ordering, are logically depicted in Figure 1, with the exception of ASUM and Clinical Data Communications which happen afterwards.

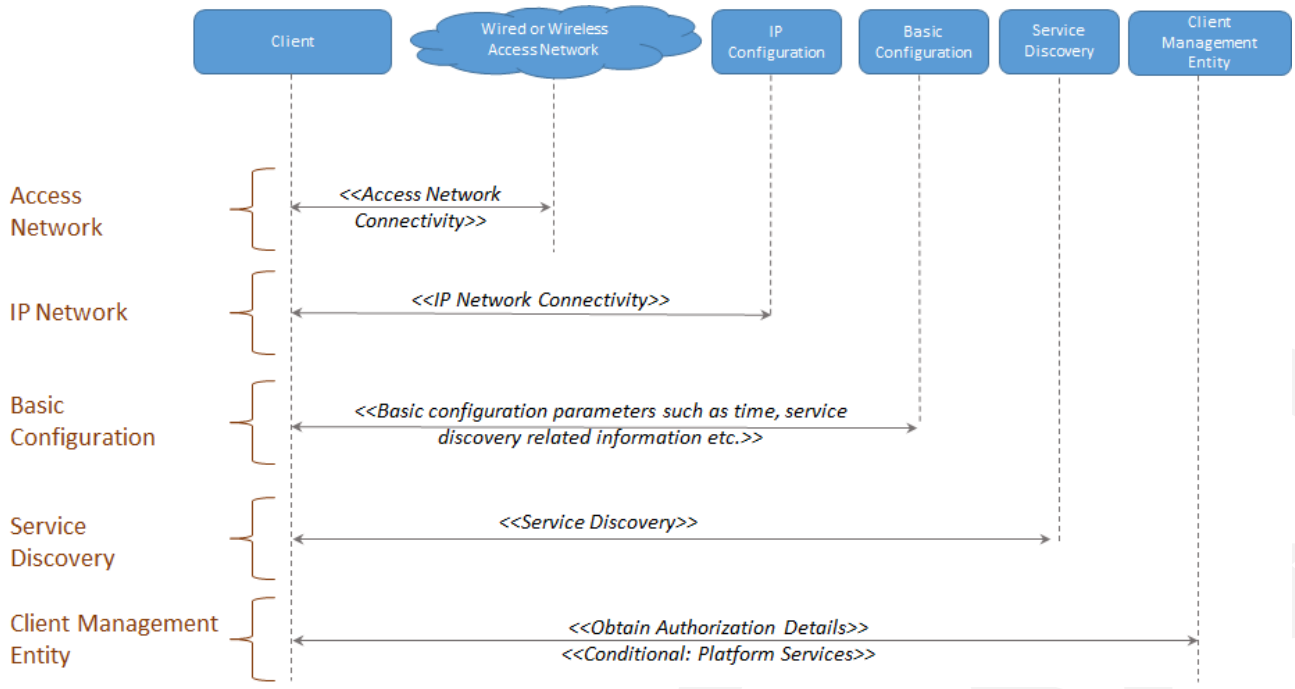

Figure 1 - High-Level Provisioning Flow

The following sub-sections illustrate the protocols and mechanisms leveraged for each of the steps, and the associated requirements.

6.2 Access Network Connectivity

6.2.1 ANC Requirement

A client that controls access network communications SHALL connect to a wired or wireless network as specified in [CMI-SP-F-ANC].

6.3 IP Network Connectivity

Once a client has connected to an access network, it must obtain an IP address for care related communications on an IP network.

6.3.1 DHCPv4 Requirement

A client that communicates via an IPv4 network and has responsibility to obtain its IP address SHALL use [IETF-RFC2131].

6.3.2 DHCPv6 Requirement

A client that communicates via an IPv6 network and has responsibility to obtain its IP address SHALL use [IETF-RFC3315].

6.3.3 IPv6-v4 Fallback Requirement

If a client that has responsibility to obtain its IP address supports both IPv4 and IPv6, then the client SHALL prioritize IPv6. If a client that has responsibility to obtain its IP address supports both IPv4 and IPv6, then the client SHALL fallback to IPv4 if IPv6 access is unavailable.

6.4 Basic Configuration

6.4.1 Basic Configuration Intro

A client is also responsible for obtaining specific, additional information during initialization: NTP server address, domain name server address, and the domain name. These are all obtained via DHCP. A client requests these additional options during the DHCP process.

6.4.2 DHCPv4 Request Requirement

For DHCPv4, the client SHALL request DHCP options #42 (NTP server), #6 (DNS Server), and #15 (domain name).

6.4.3 DHCPv6 Request Requirement

For DHCPv6, the client SHALL request DHCP options specified in [IETF-RFC5908] (NTP), [IETF-RFC3646] (DNS), and [IETF-RFC4704] (domain name).

6.4.4 Missing DHCP Options Requirement

In the presence of multiple DHCP responses, the client selects one that provides the required options as specified in [IETF-RFC2131] or [IETF-RFC3315]. If one or more of the options are not provided, then the client SHALL treat it as a failure in the DHCP process.

6.5 Service Discovery

6.5.1 Service Discovery Intro

For this version of the document, service discovery identifies one connected component: the client management entity. To keep this process lightweight, the client leverages parameters obtained via DHCP and DNS resolution.

6.5.2 Management Entity Discovery Requirement

The client SHALL discover the client management entity using the host name specified below, in conjunction with the domain name obtained via DHCP to create a fully qualified domain name and attempt to resolve it via the DNS server(s) provided during the DHCP process:

CMI_CLIENT_MGMT.<domain or subdomain name obtained via DHCP>

6.6 Provisioning Flow

6.6.1 Provisioning Flow Requirement

In accordance with the prior sub-sections, the client SHALL follow the steps specified in Figure 2 in the order shown (top to bottom). This diagram redraws Figure 1 with additional clarity based on the chosen protocols. Another view is presented in Figure 3, as stages of progression.

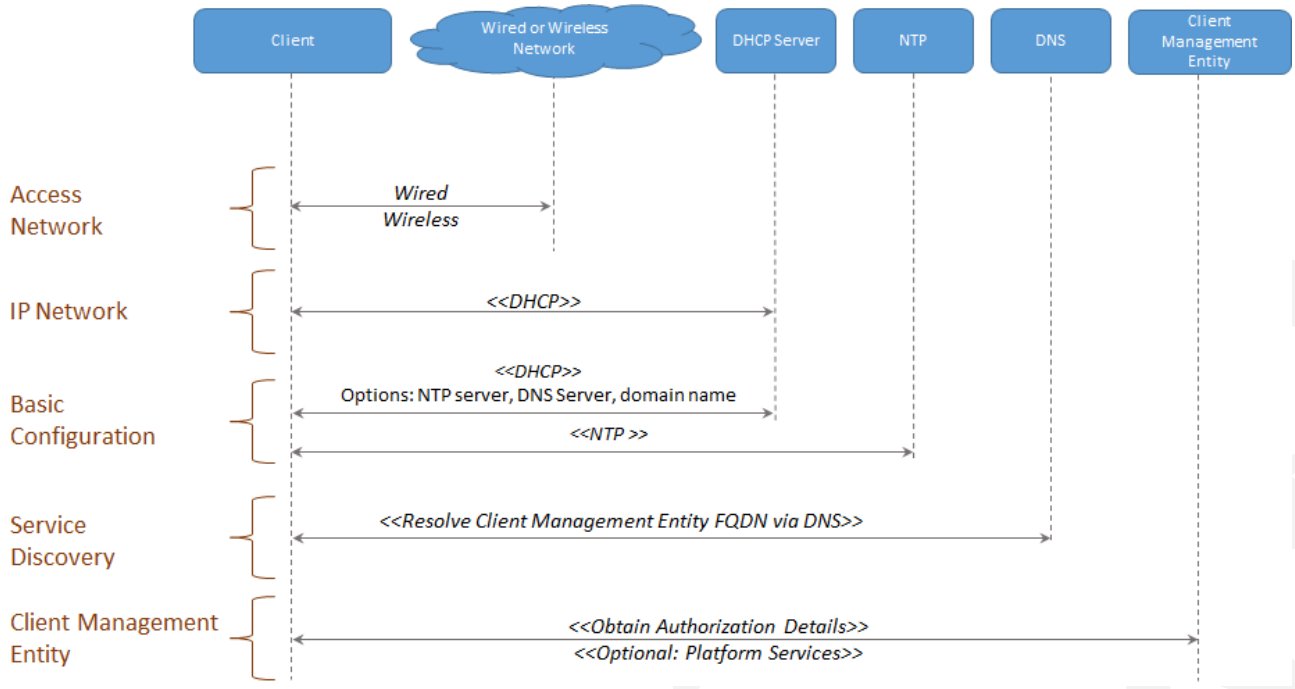

Figure 2 - Provisioning Flow Specifics

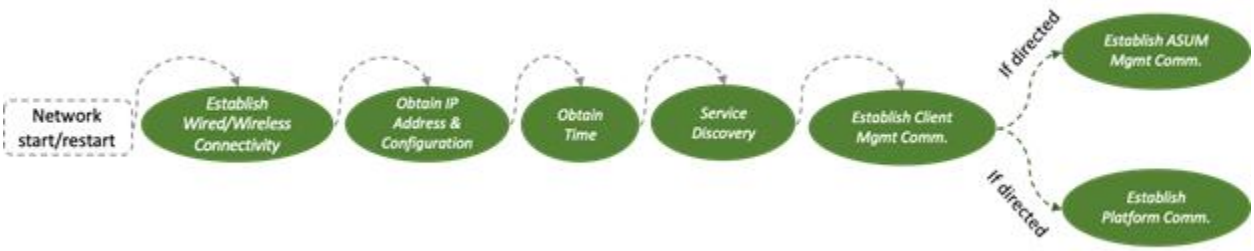

Figure 3 - Client Provisioning Flow Steps

6.7 Communication with the Client Management Entity

6.7.1 Initial Communication Requirement

Once the client resolves the Client Management Entity IP address, it SHALL attempt communication to verify if it is authorized or not.

6.7.2 Client Management Entity Response to Initial Communication

In its response, the Client Management Entity will indicate the following:

- Authorized | Unauthorized | Other
- ASUM Management Entity FQDN and port (if authorized)
- Clinical Data Exchange FQDN and port (if authorized)

6.7.3 ASUM Resolution Requirement

Upon receipt of an ASUM Management Entity FQDN, the Client SHALL resolve it via DNS and attempt the ASUM process [CMI-SP-F-ASUM].

6.7.4 Clinical Data Exchange Resolution Requirement

Upon receipt of a Clinical Data Exchange FQDN, the Client SHALL resolve it via DNS for clinical data communications. The specific process for this will be specified by the clinical data interoperability specifications [CMI-SP-CDI-IHE-PCD-SSE].

6.7.5 Client Behavior when Unauthorized/Deauthorized

If the CME indicates that a client is unauthorized, the client SHOULD NOT register a provisioning failure or continue the backoff-retry process. The client SHOULD maintain communication with the CME and wait to be authorized.

6.8 Minimum Connected Component Profile (MCCP)

6.8.1 Minimum Connected Component Profile (MCCP) Intro

To enable automated recognition of interoperability, the CMI architecture utilizes the MCCP.

6.8.2 Client MCCP Requirement

Whenever a client establishes, or reestablishes, communication with a client management entity or platform service, it SHALL present its minimum connected component profile (MCCP) as specified in [CMI-SP-F-ID].

6.8.3 CME MCCP Requirement

Whenever a client management entity establishes communication with a client, it will present its minimum connected component profile (MCCP) as specified in [CMI-SP-F-ID].

7 Client Resiliency

7.1 Client Resiliency Intro

Provisioning depicts the ideal client provisioning flow, without any errors. This cannot always be expected during deployment and operations. Connected components can fail or encounter errors not only during the provisioning flow, but while transmitting clinical data, updating software, or performing other functions. To ensure automated interoperability, the connected components need to identify errors and be prepared to recover automatically (to minimize manual intervention) and efficiently (e.g., without exacerbating the error conditions).

This section addresses such resiliency requirements for clients. Specifically, it provides a uniform mechanism for automated recovery. The specific conditions that clients should identify, log, and report (when possible) are specified as part of Management.

Automated recovery is based on retry and backoff mechanisms. Retry mechanisms ensure that the connected components can attempt to recover without manual intervention. Backoff ensures that retries are "spaced out" and don't contribute to, or amplify, message avalanche scenarios.

7.2 Retry and Backoff Algorithm

7.2.1 Retry and Backoff Algorithm Intro

The following backoff and retry algorithm is specified for use by clients. For the sake of simplicity and uniformity, it is expected to be reused across error conditions. However, to ensure that clients from the same manufacturer do not behave in an identical manner and retry at the exact same time, a client-specific pseudo-random timer is specified. In addition, the concept of a 'macro timer' is introduced that governs the overall process, such as the provisioning flow, to ensure that the retries are not ad infinitum.

- While 'macro timer' has not expired, retry once, 1 second later
    - If <desired outcome> is successful: exit
    - If unsuccessful;
        - START [Backoff & Retry]
            - While 'macro timer' has not expired:
                - wait for a pseudo-random delay period between (1..10 secs)
                - while <desired outcome> is unsuccessful
                    - <Retry 6 times at these intervals: 1, 2, 3, 5, 8, 11 secs >

- Go to START

7.2.2 Backoff and Retry Requirement

The client SHALL use the above algorithm whenever a failure occurs, and for each such failure. For instance, if a client encounters a DHCP failure and a DNS failure during the same provisioning flow, then it will invoke the above algorithm twice, once for DHCP and one for DNS.

7.2.3 Random Seed Requirement

Each client from the same manufacturer SHALL attempt a distributed pseudo-random delay via the use of a semi-unique random seed, such as a number from its identifier (e.g., mac address). A successful implementation of this requirement can be observed by making sure that two models from the same manufacturer do not backoff using the same delay times upon encountering an error.

7.2.4 Macro Timer

The macro timer above is specific to each macro process (e.g., provisioning flow, ASUM etc.) with defaults specified in the corresponding sub-sections. They may also be configured with different values, where supported.

7.3 Provisioning Flow Resiliency

7.3.1 Provisioning Flow Macro Timer with Control Requirement

Clients may or may not have control over provisioning steps, such as access network connectivity and DHCP. If it does have control over these processes, the client SHALL initiate a macro timer, t0A, with a default value of 120 seconds when it initiates the provisioning flow and follow the steps, including backoff and retry mechanism, as illustrated in Figure 4.

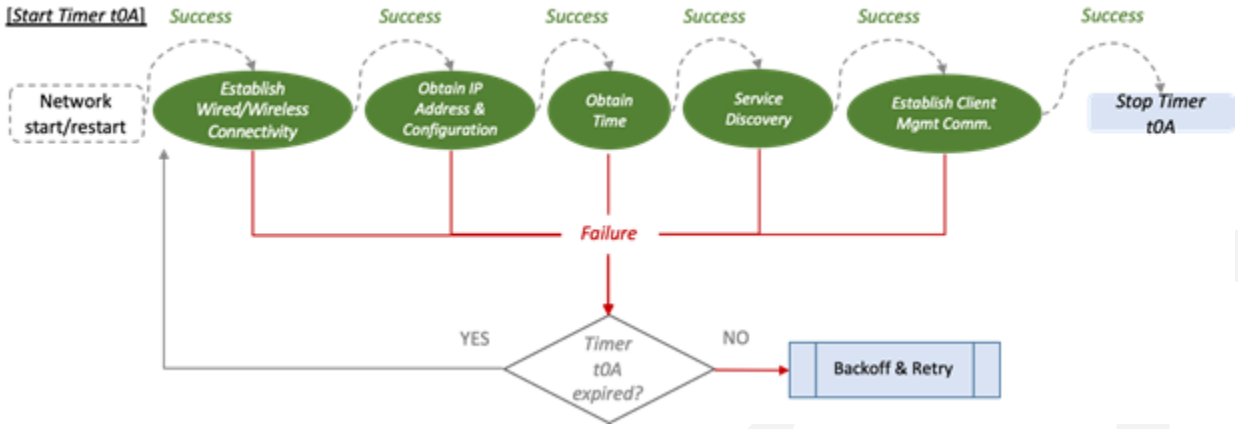

Figure 4 - Client Provisioning Flow with Error States

7.3.2 Provisioning Flow Macro Timer without Control Requirement

If a client does not have control over these processes, the client SHALL initiate a macro timer, t0B, with a default value of 60 seconds when it initiates the provisioning flow and follow the steps, including backoff and retry mechanism, as illustrated in Figure 5.

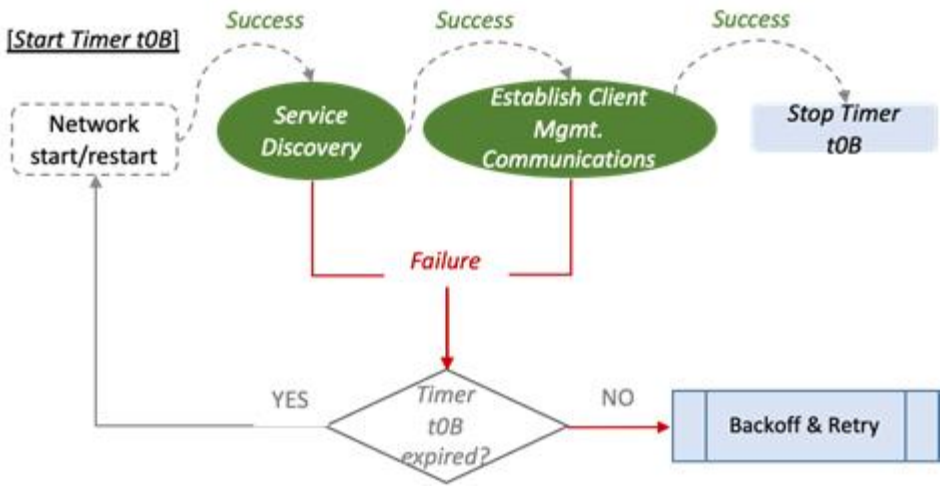

Figure 5 - Client Provisioning Flow with Error States

7.4 ASUM Management Entity Resiliency

7.4.1 ASUM Management Entity Macro Timer Requirement

The client SHALL initiate a macro timer, t1, with a default value of 240 seconds when it initiates communication with the ASUM management entity.

7.4.2 ASUM Management Entity Retry and Backoff Requirement

If an error is encountered that prevents the successful completion of a stage, the client SHALL utilize the backoff and retry mechanism as illustrated in Figure 6.

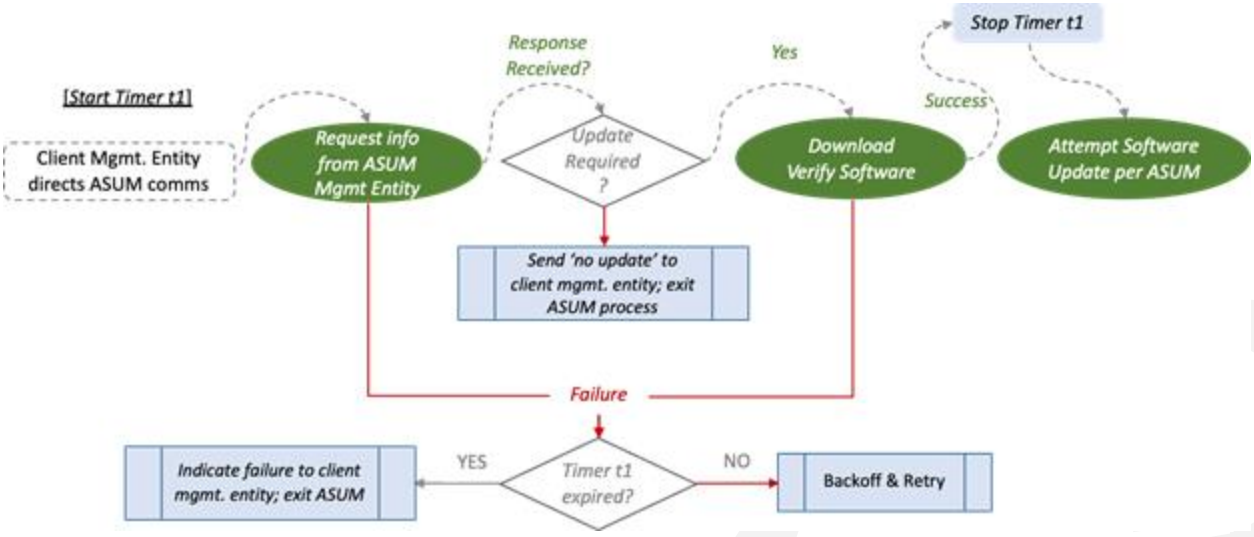

Figure 6 - ASUM Process with Error States

7.5 Clinical Data Exchange Communications Resiliency

7.5.1 Clinical Data Exchange Communications Macro Timer Requirement

The client SHALL initiate a macro timer, t2, with a default value of 60 seconds when it initiates communication with the Clinical Data Exchange.

7.5.2 Clinical Data Exchange Communications Retry and Backoff Requirement

If an error is encountered that prevents the successful completion of a stage, the client SHALL utilize the backoff and retry mechanism as illustrated in Figure 7.

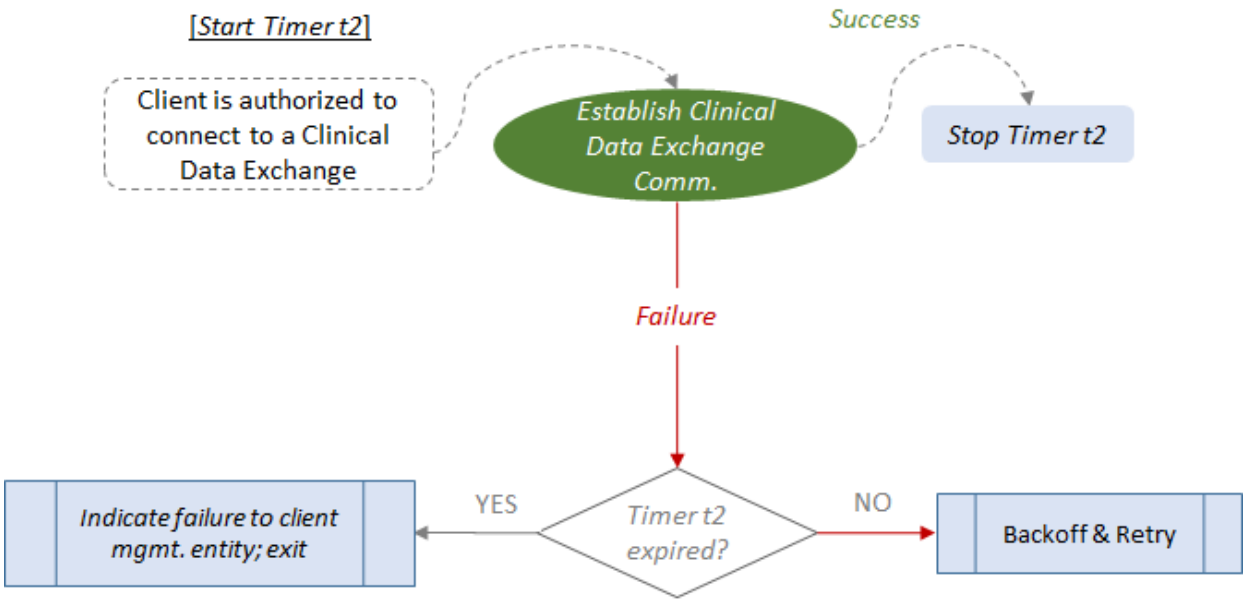

Figure 7 - Clinical Data Exchange Communication Process with Error States

7.6 Client Data Transmission Resiliency

7.6.1 Client Data Transmission Macro Timer Requirement

The client SHALL initiate a macro timer, t3, with a default value of 60 seconds when it initiates data transmission.

7.6.2 Client Data Transmission Retry and Backoff Requirement

If an error is encountered that prevents the successful completion of a stage, the client SHALL utilize the backoff and retry mechanism as illustrated in Figure 8.

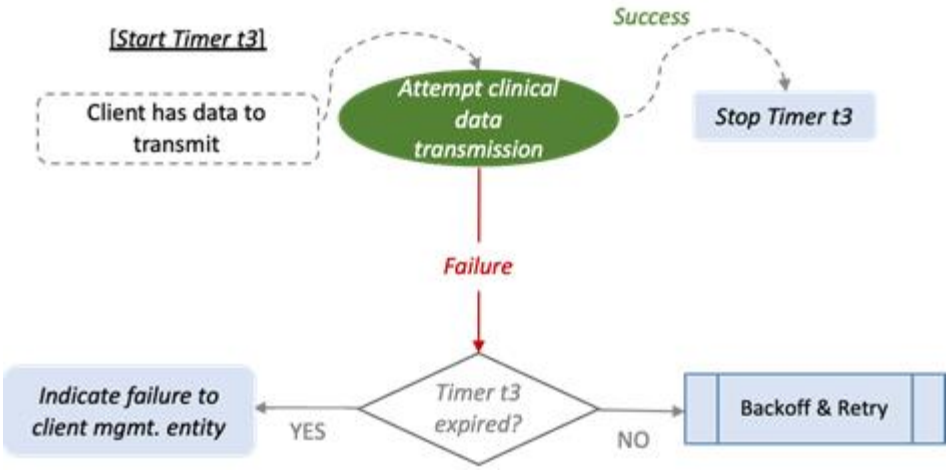

Figure 8 - Client Data Transmission Process with Error States

8 Management

8.1 Management Intro

Management broadly refers to architectural capabilities that allow technical operations personnel to ensure efficient operations. These include, but are not limited to:

- Event management for monitoring of connected component and network operations, described in this section
- Macro functionality, such as secure software update, addressed in [CMI-SP-F-ASUM]
- Configuration of connected components, which is unaddressed with the exception of minimal configuration

The following sub-sections provide a framework for event management, and ways in which it can be leveraged for resiliency efforts.

8.2 Events & Event Code Format

8.2.1 Events & Event Code Format Intro

Events, in this context, are specific conditions that are primarily identified to ensure recovery. When these events occur, they are stored via local logs to ensure that technical operations personnel are informed and can take corrective action. They are also transmitted to the management entity when possible. To provide a uniform way to record events, a format is specified in Table 1. All CMI specified events will use this format.

8.2.2 Log Format Requirement

A Client SHALL log events using the format specified in Table 1.

Table 1 - Code Format

FORMAT	< Specifier>-< type>-<category>-<identifier>-<Optional Text>
SPECIFICS	["CMI"|"CMI_V_<vendor-specific-identifier>"]-["S"|"E"|"W"|"I"]-["ASUM"|"CDI"|"ANC"]-[00000-99999]-[<Addl Info>]
DESCRIPTION	SPECIFIER ☞ CMI = CMI-specified codes| <vendor-specific unique identifier> (codes not specified by CMI) TYPE ☞ S = Success | E = Error | W = Warning | I = Informational CATEGORY ☞ ANC = Access Network Connectivity PF | DHCP | NTP | DNS = Provisioning Flow, PF related events CME = Client Management Entity ASUM = Automated Secure Update Mechanism CDT = Clinical Data Transmission IDENTIFIER ☞ XXXXX = number corresponding to a specific event OPTIONAL TEXT ☞ Additional information
EXAMPLE	CMI-S-PF-00000 refers to "Provisioning Flow completed successfully"

8.3 Events, Logging, and Reporting

8.3.1 Event Logging Requirement

Annex A identifies a set of events to address the different macro processes such as provisioning flow, client management communications, etc. The Client SHALL identify and log events specified in Annex A.

8.3.2 CME Event Transmission Requirement

For events that are logged after Client Management Entity (CME) communications have been established, the Client SHALL transmit them to the CME. The mechanism to transmit these will be specified by clinical data communications specifications.

9 Annex A CMI Events

9.1 CMI Specified Events Intro

This normative Annex provides a set of events and their descriptions in support of the format specified in Table 1. They are categorized into the following macro-areas: provisioning flow, client management entity communications, and clinical data transmission. Other documents (e.g., ASUM) or future efforts may provide additional events.

9.2 Annex A.1 Provisioning Flow Events

CATEGORY	TYPE	ID	ADDITIONAL DETAILS	OPTIONAL TEXT	NEXT STEPS
PF	S	00000	Provisioning Flow completed successfully	none	Initiate clinical data communications
ANC	W	00012	Cannot connect to network, initiating backoff/retry	"Wired|Wireless;" <share any additional details>	Backoff/retry (for wireless with secondary SSIDs)
ANC	E	00015	Resetting while trying to connect to network due to timer t0 expiration	"Wired|Wireless;" <share any additional details>	Soft reset of client; reset t0
ANC	E	00019	Unrecoverable error while connecting to network, resetting prior to timer t0 expiration	"Wired|Wireless;" <share any additional details>	Soft reset of client; reset t0
DHCP	W	00020	Cannot obtain information from DHCP, initiating backoff/retry	"DHCPv4|DHCPv6;" <share any additional details>	Backoff/retry
DHCP	E	00025	Resetting while trying to connect to network due to timer t0 expiration	"DHCPv4|DHCPv6;" <share any additional details>	Soft reset of client; reset t0
DHCP	E	00029	Unrecoverable error during DHCP, soft reset prior to timer t0 expiration	"DHCPv4|DHCPv6;" <share any additional details>	Soft reset of client; reset t0
NTP	W	00030	Cannot obtain time from NTP server, initiating backoff/retry	<NTP Server Address>; share available details	Backoff/retry with the next address if available
NTP	E	00035	Resetting while obtaining time due to timer t0 expiration	<NTP Server Address>; share available details	Soft reset of client
NTP	E	00039	Unrecoverable error while obtaining time, soft reset prior to timer t0 expiration	<NTP Server Address>; share available details	Soft reset of client; reset t0

CATEGORY	TYPE	ID	ADDITIONAL DETAILS	OPTIONAL TEXT	NEXT STEPS
DNS	W	00042	Cannot resolve Clinical Data Exchange FQDN from DNS, initiating backoff/retry	<DNS IP>,<Clinical Data Exchange FQDN>; <share any additional details>	Backoff/retry with the next DNS IP (if available)
DNS	E	00045	Resetting while resolving Clinical Data Exchange FQDN from DNS due to timer t0 expiration	<DNS IP>,<Clinical Data Exchange FQDN> <share any additional details>	Soft reset of client
DNS	E	00048	Fatal error while resolving Clinical Data Exchange FQDN from DNS, soft reset prior to timer t0 expiration	<DNS IP>,<Clinical Data Exchange FQDN> <share any additional details>	Soft reset of client
DNS	W	00050	Cannot resolve Management FQDN from DNS, initiating backoff/retry	<DNS IP>,<MGMT FQDN>; <share any additional details>	Backoff/retry with the next DNS IP (if available)
DNS	E	00055	Resetting while resolving Management FQDN from DNS due to timer t0 expiration	<DNS IP>,<MGMT FQDN> <share any additional details>	Soft reset of client
DNS	E	00058	Fatal error while resolving Management FQDN from DNS, soft reset prior to timer t0 expiration	<DNS IP>,<MGMT FQDN> <share any additional details>	Soft reset of client
DNS	W	00050	Cannot resolve ASUM Management FQDN from DNS, initiating backoff/retry	<DNS IP>,<ASUM MGMT FQDN>; <share any additional details>	Backoff/retry with the next DNS IP (if available)
DNS	E	00055	Resetting while ASUM Management FQDN from DNS due to timer t0 expiration	<DNS IP>,<ASUM MGMT FQDN> <share any additional details>	Soft reset of client
DNS	E	00058	Fatal error while ASUM Management FQDN from DNS, soft reset prior to timer t0 expiration	<DNS IP>,<ASUM MGMT FQDN> <share any additional details>	Soft reset of client

9.3 Annex A.2 Client Management Entity Communications Events

CATEGORY	TYPE	ID	ADDITIONAL DETAILS	OPTIONAL TEXT	NEXT STEPS
CME	S	00100	Connected to the Clinical Data Exchange (MCCP exchanged, interoperable)	<MGMT FQDN>, <MGMT IP>	None
CME	E	00101	Connected to the Clinical Data Exchange (MCCP exchanged, not interoperable)	<MGMT FQDN>,<MGMT IP>; <Client Release Bundle>, <MGMT Release Bundle> <share any additional details>	Backoff/retry; try with next MGMT IP if available
CME	E	00102	No response from the Management Entity, initiating backoff/retry	<MGMT FQDN>,<MGMT IP>; <share any additional details>	Backoff/retry; try with next MGMT IP if available
CME	E	00110	Client authentication to Management Entity failed	<MGMT FQDN>,<MGMT IP>; <share any additional details>	Backoff/retry; try with next MGMT IP if available
CME	E	00120	Management Entity authentication to Client failed	<MGMT FQDN>,<MGMT IP>; <share any additional details>	Backoff/retry; try with next MGMT IP if available
CME	E	00130	Secure communications could not be initiated (catch-all, and outside of other explicit errors)	<MGMT FQDN>,<MGMT IP>; <share any additional details>	Backoff/retry; try with next MGMT IP if available
CME	W	00140	Management Entity communication failed; retrying data over same secure communications link	<MGMT FQDN>,<MGMT IP>; <share any additional details>	Backoff/retry over the same secure connection
CME	E	00145	Management entity secure communications link failed; reestablishing secure communications link	<MGMT FQDN>,<MGMT IP>; <share any additional details>	Reestablish security link
CME	E	00149	Unrecoverable error during communications with Management entity	<MGMT FQDN>,<MGMT IP>; <share any additional details>	Soft reset of client
CME	W	00151	Deauthorized from the Clinical Data Exchange	<share any additional details>	Wait for authorization; backoff/retry as required

9.4 Annex A.3 Clinical Data Transmission Events

CATEGORY	TYPE	ID	ADDITIONAL DETAILS	OPTIONAL TEXT	NEXT STEPS

CATEGORY	TYPE	ID	ADDITIONAL DETAILS	OPTIONAL TEXT	NEXT STEPS
CDT	S	00200	Connected to the Clinical Data Exchange (MCCP exchanged; interoperable)	<Clinical Data Exchange FQDN>, <Clinical Data Exchange IP>	None
CDT	E	00201	Connected to the Clinical Data Exchange (MCCP exchanged; not interoperable)	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <Client Release Bundle>, <Clinical Data Exchange Release Bundle> <share any additional details>	Backoff/retry; try with next Clinical Data Exchange IP if available
CDT	W	00202	No response from the Clinical Data Exchange, initiating backoff/retry	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Backoff/retry; try with next Clinical Data Exchange IP if available
CDT	E	00210	Client authentication to Clinical Data Exchange failed	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Backoff/retry; try with next Clinical Data Exchange IP if available
CDT	E	00220	Clinical Data Exchange authentication to Client failed	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Backoff/retry; try with next Clinical Data Exchange IP if available
CDT	E	00230	Secure communications could not be initiated (catch-all, and outside of other explicit errors)	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Backoff/retry; try with next Clinical Data Exchange IP if available
CDT	W	00240	Clinical Data Exchange data communication failed; retrying data over same secure communications link	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Backoff/retry over the same secure connection
CDT	E	00245	Clinical Data Exchange secure communications link failed; reestablishing secure communications link	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Reestablish security link
CDT	E	00249	Unrecoverable error during communications with Clinical Data Exchange	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Soft reset of client
CDT	W	00251	Disconnected from the Clinical Data Exchange due to Management Entity Deauthorization	<Clinical Data Exchange FQDN>,<Clinical Data Exchange IP>; <share any additional details>	Wait for authorization; backoff/retry as required

10 Annex B Secure Transport Using TLS

10.1 Annex B Secure Transport Using TLS Intro

This section presents requirements for securing transport via TLS. Two interfaces are considered, one used by clients and the other by platform services, applications, and other connected components (e.g., EHRs). Interface A originates at platform services, gateways, or applications and connects towards medical devices. Implemented on a platform service, Interface A may connect to gateways or directly to medical devices. Implemented on a gateway, Interface A connects to medical devices. Gateway to gateway interfaces are not considered at this time. Interface B originates at clients and connects towards platform services. This basic architecture is illustrated in Figure 1. Gateways may translate proprietary clinical data or can forward clinical data as-is. Proprietary messaging between medical devices and gateways, while not prohibited, is not in scope of this specification.

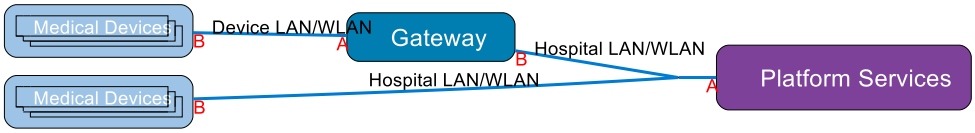

Figure B-1: Architecture TLS Interfaces

Before a client communicates with a platform service, it first establishes a secure connection using TLS. This includes mutual authentication using a device certificate, message encryption, and message authentication. If the client is a gateway that only forwards data, the TLS connection may be established between the medical device and platform service through the gateway, similar to a tunnel. This functionality is out of scope for this draft.

A certificate (issued by the CMI PKI) is used for mutual authentication between connected components. Certificate hierarchy, profile, registration, and acquisition details are defined in [CMI-SP-F-CP]. This specification assumes equivalent functional behaviors from clients regardless of secure transport implementation.

10.2 Secure Transport Using TLS Requirements

10.2.1 Cryptographic Requirements for All Connected Components

10.2.1.1 ECC Curve Support Requirement

Connected Components that support ECC cryptography SHALL support NIST curves [FIPS-186-4] and MAY support additional curves with similar or stronger security.

10.2.1.2 RSA Key Size Requirement

Connected Components that support RSA cryptography SHALL support RSA keys up to 4096 bits for certificate validation and keys up to 2048 bits for signatures.

10.2.1.3 Algorithm Support Requirement

Connected Components SHALL support the SHA-2 hashing algorithm family (e.g., SHA-256, SHA-384, and SHA-512) [FIPS-180-4] and MAY support other hashing algorithms with better or similar security. Connected Components SHALL support AES with key sizes of 128 bits.

10.2.2 Authentication Requirements for All Connected Components

10.2.2.1 TLS Version Requirement

Connected Components SHALL support TLS version 1.2 and MAY also support higher versions. Connected Components SHALL NOT use a TLS protocol version lower than 1.2 on CMI specified interfaces.

10.2.2.2 Trust Anchor Requirement

For each supported cryptographic scheme, the ECC or RSA root CA certificates defined in The Center's Certificate Policy and authorized by The Center SHALL be installed in a Connected Component as trust anchors for validating received Connected Component certificates.

10.2.2.3 Issuing Certificate Requirement

During TLS authentication messaging, a Connected Component SHALL include the issuing CA certificate with its own certificate in the TLS Certificate message.

10.2.2.4 Basic Path Validation Requirement

A Connected Component SHALL validate certificates that it receives using Basic Path Validation procedures defined in the X.509 PKI certificate standard [IETF-RFC5280]. If a Connected Component cannot validate the received certificates, it SHALL reject authentication, log an error, and close the connection.

10.2.2.5 Response for Revoked Certificate Requirement

If a certificate has been revoked or if its revocation status is unknown, a Connected Component SHALL reject authentication, log an error, and follow failure paths defined by resiliency requirements.

10.2.2.6 Authenticity and Freshness Requirement

OCSP Responses and CRLs SHALL be validated by a Connected Component for authenticity and freshness before they can be used to check the revocation status of a certificate.

10.2.2.7 Key Storage Requirement

A Connected Component SHALL store the certificate private key in a manner that deters unauthorized disclosure and modification. A Connected Component SHALL meet security

requirements for all instances of private and public permanent key storage according to [CMI-SP-F-ID].

10.3 B.1 Interface A: Southbound from Connected Components

10.3.1 Interface A Intro

Interface A may be implemented by platform services, gateways, or applications.

10.3.2 Cryptographic Requirements for Connected Components supporting Interface A

10.3.2.1 TLS Version Selected By Interface A

Connected Components implementing Interface A will be configured to select what TLS protocol version is used during the TLS message exchange.

10.3.2.2 Interface A RSA ECC Support Requirement

Connected Components implementing Interface A SHALL support both elliptic curve (ECC) and RSA public key cryptography for certificate processing and key exchange to provide interoperability with clients that support one or both cryptographic schemes.

10.3.2.3 Interface A Algorithm Support Requirement

Connected Components implementing Interface A SHALL support ECDHE and DHE algorithms for secure key exchange. Connected Components implementing Interface A SHALL support AES with key size 256 bit.

10.3.3 Authentication Requirements for Connected Components supporting Interface A

10.3.3.1 Interface A Mandatory Cipher Requirement

Connected Components implementing Interface A SHALL support the following TLS cipher suites for interface A. Connected Components implementing Interface A SHALL select a cipher from the Client Hello using the preference-ordered cipher list shown in Table B-1.

Table B-1: Mandatory Cipher Suite List for Interface A

Cipher Suite	Reference
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	[IETF-RFC5289]
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	[IETF-RFC5288]
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	[IETF-RFC5289]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	[IETF-RFC5246]
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	[IETF-RFC8422]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	[IETF-RFC5246]

10.3.3.2 Interface A Optional Ciphers Requirement

Connected Components implementing Interface A MAY support TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, which uses both ECC and RSA public key cryptography. If this cipher suite is supported, a Connected Component's preference-ordered cipher list for interface A SHALL be modified as shown in Table B-2.

Table B-2: Optional Cipher Suite List for Interface A

Cipher Suite	Reference
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	[IETF-RFC5289]
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	[IETF-RFC5288]
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	[IETF-RFC5289]
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	[IETF-RFC5289]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	[IETF-RFC5246]
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	[IETF-RFC8422]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	[IETF-RFC5246]

10.3.3.3 Interface A Certificate Selection Requirement

Connected Components implementing Interface A SHALL select the certificate to be used for the TLS connection based on the authentication scheme of the selected cipher. For example, for ciphers that use ECDSA, the ECC certificate will be sent in the Certificate message by the Connected Component. On the other hand, for ciphers that use RSA, the RSA certificate will be sent in the Certificate message by the Connected Component.

10.3.3.4 Interface A Basic Path Validation Requirement

During Basic Path Validation procedures, a Connected Component implementing Interface A SHALL verify that the device identifier value in the Common Name attribute of the Subject field is authorized to connect.

10.3.3.5 Interface A Revocation Check Requirement

When a Connected Component implementing Interface A validates received certificates, it SHALL check their revocation status and the revocation status of every certificate in the certificate's chain up to (but excluding) the Root CA. Two different revocation status checking mechanisms SHALL be supported: OCSP (preferred mechanism) and CRL (backup mechanism). The following revocation requirements apply:

10.3.3.5.1 Interface A CRL Requirement

The latest version of the CRLs signed by The Center's root CA and a Tier 2 sub-CA SHALL be installed during setup on any Connected Component implementing Interface A. A Connected Component implementing Interface A SHALL attempt to update these CRLs before they expire using the distribution server URL in the CRL header.

10.3.3.5.2 Interface A OCSP Requirement

When performing certificate validation, a Connected Component implementing Interface A SHALL check revocation status using OCSP [IETF-RFC6960]. If the OCSP responses are not provided via the TLS handshake and they are not available in the local cache, a Connected Component implementing Interface A SHALL retrieve a response from the OCSP server URLs found in the received certificate and the received CA certificate. If the OCSP URL is not available (e.g., not present in the certificate to be validated or not locally configured), a Connected Component SHALL use the CRL. Also in this case, a Connected Component implementing Interface A SHOULD retrieve the CRL from the URL specified in the certificates that are being validated (i.e., in the cRLDistributionPoints extension) and MAY retrieve the CRL from a local cache, if available.

10.3.3.6 Interface A TLS Stapling Requirement

A Connected Component implementing Interface A SHALL support TLS Stapling [IETF-RFC6961] for providing OCSP revocation status of its certificates to other Connected Components. The Connected Component implementing Interface A forwards OCSP requests to the CA OCSP server URL embedded in its server certificate and forwards OCSP responses via the initial TLS message exchange.

10.4 B.2 Interface B: Northbound from Connected Component

10.4.1 Interface B Intro

Interface B may be implemented by medical devices or gateways.

10.4.2 Cryptographic Requirements for Connected Components supporting Interface B

10.4.2.1 Interface B RSA ECC Support Requirement

Connected Components implementing Interface B SHALL support one of RSA and ECC cryptography schemes for certificate validation procedures. To promote interoperability across systems, Connected Components implementing Interface B MAY support both cryptography schemes.

10.4.2.2 Interface B Algorithm Support Requirement

Connected Components implementing Interface B SHALL support one of ECDHE and DHE algorithms for secure key exchange. Connected Components implementing Interface B SHOULD support AES with key size 256 bits.

10.4.3 Authentication Requirements for Connected Components supporting Interface B

10.4.3.1 Interface B TLS Requirement

A Connected Component supporting Interface B SHALL establish a secure TLS [IETF-RFC5246] connection to be used for exchanging messages. A Connected Component supporting Interface B SHALL initiate the TLS connection.

10.4.3.2 Interface B RSA Cipher Requirement

If a Connected Component implementing Interface B supports RSA cryptography, it SHALL support at least one the following TLS cipher suites:

Table B-3: RSA Cipher Suite List for Interface B

Cipher Suite	Reference
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	[IETF-RFC5246]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	[IETF-RFC5246]
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	[IETF-RFC5288]

If a Connected Component implementing Interface B supports more than one cipher from this list, it SHALL present them with the priority shown in the above list.

10.4.3.3 Interface B ECC Cipher Requirement

If a Connected Component implementing Interface B supports ECC cryptography, it SHALL support at least one of the following TLS cipher suites:

Table B-4: ECC Cipher Suite List for Interface B

Cipher Suite	Reference
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	[IETF-RFC5289]
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	[IETF-RFC8422]
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	[IETF-RFC5289]

If a Connected Component implementing Interface B supports more than one cipher from this list, it SHALL present them with the priority shown in the above list.

10.4.3.4 Interface B Optional Cipher Requirement

A Connected Component implementing Interface B MAY support TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 [IETF-RFC5289] which uses both ECC and RSA public key cryptography. If supported, a Connected Component implementing Interface B SHALL add the cipher to the top of the list of ciphers presented in the Client Hello message.

10.4.3.5 Interface B Basic Path Validation Requirement

During Basic Path Validation procedures, a Connected Component implementing Interface B SHALL verify that the host portion of the destination URL matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the received certificate. If a Connected Component implementing Interface B cannot validate the source of the received certificates, it SHALL reject authentication, log an error, and follow failure paths defined by resiliency requirements.

10.4.3.6 Interface B OCSP Requirement

When performing certificate validation, a Connected Component implementing Interface B SHALL check revocation status of every certificate in the certificate chain by using OCSP [IETF-RFC6960] responses that are provided via OCSP Stapling [IETF-RFC6961] during the initial TLS message exchange. A Connected Component implementing Interface B SHALL also verify that the responses are correctly signed and that the certificate of the OCSP signer is properly validated. In case the revocation information is not available for every certificate in the certificate chain that is being validated, a Connected Component implementing Interface B SHALL consider the whole chain invalid, reject the authentication, log an error, and follow failure paths defined by resiliency requirements.

11 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.

Sumanth Channabasappa authored this document. Special thanks to those who were directly involved via a variety of discussions, reviews and input: **Ken Fuchs, Matthew Pekarske, Phil Raymond, Mitchell A. Ross, David Fann, Bowen Shaner,** and **Spencer Crosswy**. **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, 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
Jason Mortensen	Bernoulli Health
Jay White	Laird
Jay White	Laird
Jeffrey Brown	GE

Working Group Participants	Company Affiliation
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