CENTER *for* MEDICAL
INTEROPERABILITY

The Center for Medical Interoperability Specification Clinical Data Interoperability Based on IHE PCD – Identity & Secure Transport

CMI-SP-CDI-IHE-PCD-IST-D01-20190311

DRAFT

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-CDI-IHE-PCD-IST-D01-20190311			
Document Title:	Clinical Data Interoperability Based on IHE PCD – Identity & Secure Transport			
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.

Trademarks

Contents

1 Scope 5
1.1 Introduction and Purpose 5
1.2 Requirements 5
2 References 6
2.1 Normative References 6
2.2 Informative References 7
2.3 Reference Acquisition 7
3 Terms and Definitions 7
4 Abbreviations and acronyms 8
5 Overview 9
5.1 Architecture 9
6 Identity and Secure Transport Requirements 9
6.1 Interface A (Southbound from Platform) 10
6.2 Interface B (Northbound from Client) 12
Appendix I. Acknowledgements 14

Figures

Figure 1: Architecture showing IHE PCD HL7 Interfaces 9

1 Scope

1.1 Introduction and Purpose

This specification provides the requirements for securing Integrating the Healthcare Enterprise Patient Care Device Health Level Seven International (IHE PCD HL7) Minimum Lower Layer Protocol (MLLP) messaging between the platform and medical devices, as part of The Center's Phase 1 efforts. It covers mutual authentication of identities using a certificate public key infrastructure (PKI) managed by The Center. Traffic is secured using Transport Layer Security (TLS) with proven industry standard encryption and message authentication algorithms. These security features help protect against device spoofing, unauthorized access, information disclosure, and tampering.

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.

[IETF-RFC5246] IETF RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008

https://tools.ietf.org/html/rfc5246

[IETF-RFC5289] IETF RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), August 2008

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

[IETF-RFC5288] IETF RFC 5288, AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008

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

[IETF-RFC5280] IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

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

[IETF-RFC6960] IETF RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013

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

[IETF-RFC6961] IETF RFC 6961, The Transport Layer Security (TLS) Multiple Certificate Status Request Extension, June 2013

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

[FIPS-140-2] Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, June 2001 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[CMI-SP-F-CP] "Certificate Policy for The Center's Public Key Infrastructure", Center for Medical Interoperability.

https://medicalinteroperability.org/specifications/D01/CMI-SP-F-CP-D01-20190311.pdf

[CMI-SP-F-ANC] "Access Network Connectivity Specification", Center for Medical Interoperability.

https://medicalinteroperability.org/specifications/D01/CMI-SP-F-ANC-D01-20190311.pdf

[CMI-SP-F-ID] "Identity Overview", Center for Medical Interoperability.

https://medicalinteroperability.org/specifications/D01/CMI-SP-F-ID-D01-20190311.pdf

2.2 Informative References

This specification uses the following informative reference.

[CMI-DOC-TD] "Terms and Definitions", Center for Medical Interoperability.

https://medicalinteroperability.org/specifications/D01/CMI-DOC-TD-D01-20190311.pdf

2.3 Reference Acquisition

Center for Medical Interoperability, 8 City Boulevard, Suite 203 | Nashville, TN 37209;
Phone +1-615-257-6410; http://medicalinteroperability.org/

Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org

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
CMI	Center For Medical Interoperability
CRL	Certificate Revocation List
DHE	Diffie-Hellman Exchange
ECC	Elliptic curve
ECDHE	Elliptic curve Diffie-Hellman key exchange
EHR	Electronic Health Record
HL7	Health Level Seven International
IHE PCD	Integrating the Healthcare Enterprise Patient Care Device
MLLP	Minimum Lower Layer Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RSA	Rivest–Shamir–Adleman
TLS	Transport Layer Security

5 Overview

5.1 Architecture

Platforms, Medical Devices, and Gateways are considered connected components. Once a connected component network access, it communicates with other connected components using IHE PCD HL7 messaging and the MLLP transport protocol. The requirements for network access are defined in The Center's Access Network specification [CMI-SP-F-ANC].

Two interfaces are defined, one used by Clients and the other by Platforms or similar elements. Interface A originates at Platforms, Gateways, or other medical servers (such as EHRs) and connects towards Medical Devices. Implemented on a Platform, 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 ordinates at Clients (Medical Devices or Gateways) and connects towards Platforms. This basic architecture is illustrated in Figure 1. Gateways may translate between IHE PCD HL7 messaging and proprietary messaging or can forward IHE PCD HL7 messaging. In HL7 terminology, Interface A is Southbound and Interface B are Northbound. Proprietary messaging between Medical Devices and Gateways, while not prohibited, is not in scope of this specification.

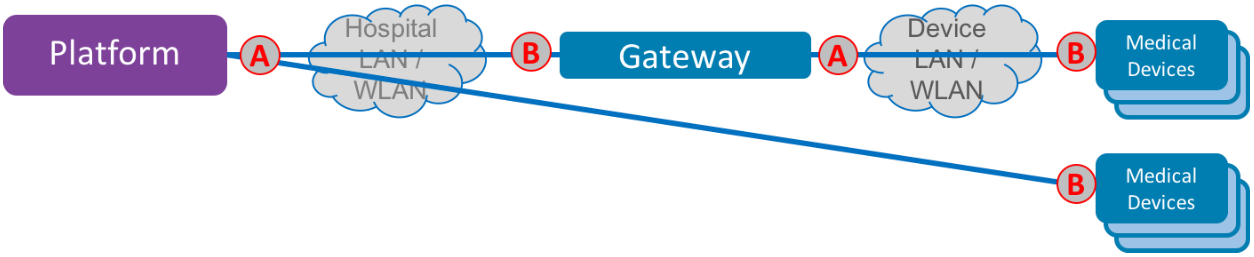

Figure 1: Architecture showing IHE PCD HL7 Interfaces

Before a Client communicates with the Platform using IHE PCD messaging 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 forwarding IHE PCD messaging, it does not establish a TLS connection with the Platform. In this case, the TLS connection is established between the Medical Device end point and the Platform, similar to a tunnel.

6 Identity and Secure Transport Requirements

The following sections define implementation requirements for connected components to establish a secure TLS connection for IHE PCD HL7 messaging using MLLP. It is a assumed that the Client has obtained network access. A certificate (issued by the CMI PKI) is used for mutual authentication of Platforms and Clients. Certificate hierarchy and profile details are defined in [CMI-SP-F-CP]. Medical device manufacturers and hospital members contact The Center to register and acquire digital certificates. This specification assumes equivalent functional behaviors from Clients whether implemented on Medical Devices and Gateways relative to implementation of secure transport for IHE PCD HL7.

6.1 Interface A (Southbound from Platform)

Interface A may be implemented on Platforms, Gateways, or similar medical servers. For purposes of this specification, Platform is used to reflect any component implementing Interface A.

A Platform establishes a secure TLS connection with the Client to be used for exchanging any IHE PCD HL7 over MLLP messages with it. The Client is expected to initiate the TLS connection.

Cryptographic Requirements. Platforms, Gateways, or similar medical servers SHALL support both RSA and ECC cryptography to provide interoperability with devices that support one or both crypto schemes. In particular, for the RSA scheme, Platforms should support RSA keys up to 4096 bits for certificate validation. For the ECC scheme, the server SHALL support NIST curves and may support additional curves with similar or stronger security. The server SHALL support ECDHE and DHE algorithms for secure key exchange. Compliant Platforms SHALL support AES with key sizes of 128 bits and 256 bit and SHALL also support the SHA-2 (i.e., SHA-256, SHA-384, and SHA-512) Hashing algorithm family and MAY support other Hashing algorithms with better or similar security.

Authentication Requirements:

1. The Platform or Gateway SHALL use a default port of 2575 for sending and receiving IHE PCD messages with TLS.

2. The Platform will be configured to select what TLS protocol version is used during the TLS message exchange. The Platform SHALL support TLS version 1.2 and MAY also support a higher version. The Platform SHALL NOT use a TLS protocol version lower than 1.2.

3. The Platform supports both elliptic curve (ECC) and RSA public key cryptography for certificate processing and key exchange. The Platform SHALL support the following TLS cipher suites. The Platform SHALL present these cipher options to the Client in this order.

    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
    - The Platform MAY support TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 which uses both ECC and RSA public key cryptography. If this cipher suite is included, it SHALL be presented in the ordered cipher options presented to the Client before TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256.

4. During TLS authentication messaging the Platform SHALL provide the full chain of certificates required for certificate validation. The certificate chain SHALL include the Platform's certificate and all intermediate CA certificates as described in TLS.

5. An ECC and RSA Platform certificate, private key, and issuing CA certificate as defined in The Center's Certificate Policy SHALL be securely installed in the Platform by the hospital member.

6. The ECC and RSA root CA certificates defined in The Center's Certificate Policy and authorized by The Center SHALL be installed in the Platform as trust anchors for validating received Connected Component certificates.

7. During TLS authentication messaging the Platform SHALL include the issuing CA certificate with its own certificate in the TLS Certificate message.

8. The Platform SHALL validate certificates received from the Connected Component using Basic Path Validation procedures defined in the X.509 PKI certificate standard [IETF-RFC5280] and verify that the device identifier value in the Common Name attribute of the Subject field is authorized to connect. If the Platform cannot validate the received certificates, it SHALL reject Connected Component authentication, log an error, and close the connection.

9. When a Platform validates certificates received from a Client 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. 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:

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

    - When performing certificate validation the Platform 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 Platform 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 Platform 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.

    - If a certificate has been revoked, the Platform SHALL reject Connected Component authentication, log an error, and close the connection

10. The Platform SHALL support TLS Stapling (RFC 6961) for providing OCSP revocation status about its certificates to the Connected Component. The Platform forwards OCSP requests to the CA OCSP server URL embedded in its server certificate and forwards OCSP responses to the Connected Component via the initial TLS message exchange.

11. The Platform SHALL store the Platform Certificate private key in a manner that deters unauthorized disclosure and modification. The Platform SHALL meet security requirements for all instances of private and public permanent key storage according to [CMI-DOC-TD]. The Platform is assumed to be operated in a trusted environment that is only accessible by authorized hospital staff.

6.2 Interface B (Northbound from Client)

Cryptographic Requirements. Relying parties implementing Northbound interfaces SHALL support one of RSA and ECC cryptography schemes for certificates' validation procedures. To promote interoperability across systems, relying parties MAY support both crypto schemes. In particular, for the RSA scheme, Platforms should support RSA keys up to 4096 bits for certificate validation and keys up to 2048 bits for signatures. For the ECC scheme, the client SHALL support NIST curves and MAY support additional curves with similar or stronger security. The relying party SHALL support one of ECDHE and DHE algorithms for secure key exchange. Any Relying party SHALL support AES with key sizes of 128 bits and SHOULD support AES with key sizes of 256 bits. Relying parties SHALL also support the SHA-2 Hashing algorithm family (e.g., SHA-256, SHA-384, and SHA-512) and MAY support other Hashing algorithms with better or similar security.

Authentication Requirements:

12. The Client SHALL establish a secure TLS [IETF-RFC5246]IETF-RFC5246 connection with a Platform to be used for exchanging any IHE PCD HL7 over MLLP messages. The Client SHALL initiate the TLS connection. The Client SHALL use a default port of 2575 for sending and receiving IHE PCD messages with TLS.

13. During the TLS message exchange the Platform will select what TLS protocol version is used. The Client SHALL support TLS version 1.2 and MAY also support a higher version. The Client SHALL NOT use a TLS protocol version lower than 1.2.

14. A Client SHALL support elliptic curve (ECC) or RSA public key cryptography cipher suites and MAY support both for certificate processing and key exchange.

    - If the Client supports RSA cryptography it SHALL support at least one the following TLS cipher suites:

        - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

        - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

        - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

- If the Client supports ECC cryptography it SHALL support at least one the following TLS cipher suites:
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- The Client MAY support TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 which uses both ECC and RSA public key cryptography.

15. An ECC or RSA root CA certificate defined in Identity Specification and authorized by The Center SHALL be installed in the Client as a trust anchor for validating received certificates.

16. During TLS authentication messaging the Client SHALL respond to a CertificateRequest message from the Platform by sending Certificate and CertificateVerify messages. The Client SHALL include the issuing CA certificate with its own certificate in the TLS Certificate message.

17. The Client SHALL validate certificates received from the Platform using Basic Path Validation procedures defined in [IETF-RFC5280][IETF-RFC5280] and verify that the host portion of the Platform URL matches the Common Name attribute of the Subject field or any domain names in the Subject Alternative Name extension in the Platform server certificate. If the Client cannot validate the received certificates, it SHALL reject Platform authentication, log an error, and periodically retry the connection

18. When a Client validates received certificates it checks their revocation status using [IETF-RFC6960]. The following revocation requirements apply to the Client:

    - When performing certificate validation the Client SHALL check revocation status of every certificate in the certificate chain by using OCSP responses that are provided by the Platform via TLS Stapling during the initial TLS message exchange. The Client SHALL check the OCSP responses for freshness (i.e., SHALL reject expired responses and MAY reject responses that are too old according to the application's policy). The Client 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, the whole chain SHALL be considered invalid and therefore the Client SHALL reject the authentication, log an error, and retry the connection at a later time.

    - If a certificate has been revoked or the revocation status is unknown, the Client SHALL reject Platform authentication, log an error, and periodically retry the connection

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

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.

Stuart Hoggan authored this document, with edits by **Steve Goeringer**. Special thanks to the following who were directly involved via a variety of discussions, reviews and input: **Ken Fuchs, JF Lancelot**, **Kai Hassing** and **Paul Schluter**.

This effort was conducted within the **Center's Architecture and Requirements** and **Security** working groups, 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**
Ali Nakoulima	Cerner
Andrew Dobbing	Laird
Barry Brown	Mortara
Bill Hagestad	Smiths Medical
Bill Pelletier	GE
Bo Dagnall	HPE
Bruce Friedman	GE Healthcare
Corey Spears	Infor
Damon Herbst	Cerner
Doug Bogia	Intel
Doug Smith	Laird
Eldon Metz	Innovision Medical
Erik Eckman	Microsoft
Guy Johnson	Zoll
Jay White	Laird
Jeff Brown	GE
JF Lancelot	Airstrip
John Zaleski	Bernoulli Health

WG Participant	**Company Affiliation**
Dr. Jorg-Uwe Meyer	MT2IT
Kai Hassing	Philips
Ken Fuchs	Draeger
Kurt Elliason	Smiths Medical
Dr. Max Pala	CableLabs
Peter Housel	Masimo
Scott Eaton	Mindray
Song Chung	Welch Allyn
Soundharya Nagasubramanian	Welch Allyn
Stefan Karl	Philips
Stuart Hoggan	CableLabs

- *Steve Goeringer (Editor, Security Working Group Lead), Sumanth Channabasappa (Architecture & Requirements Working Group Lead), David Fann, Trevor Pavey; and, Ed Miller (CTO) -- The Center*