Center for Medical Interoperability
SPECIFICATION

HEALTHCARE TRUST PLATFORM TECHNICAL SPECIFICATION

C4MI-SP-WIP-01-20191130

DRAFT

Notice

This technical specification is the result of a cooperative effort undertaken at the direction of The Center for Medical Interoperability, for the benefit of its members and its vendors. 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.

Distribution of this document is restricted pursuant to the terms of separate access agreements negotiated with each of the parties to whom this document has been furnished.

CAUTION

This document contains proprietary, confidential information that is the exclusive property of The Center. If you do not have a valid agreement with The Center for the use of this document, or have not signed a non-disclosure agreement with The Center, then you received this document in an unauthorized manner and are not legally entitled to possess or read it.

Use, duplication, and disclosure are subject to restrictions stated in your agreement with The Center.

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:	C4MI-SP-WIP-01-20191130			
Document Title:	HEALTHCARE TRUST PLATFORM TECHNICAL SPECIFICATION			
Revision History:	WIP01 – 11/30/19			
Date:	Nov 30, 2019			
Status:	**Work in Progress**	~~Draft~~	~~Issued~~	~~Closed~~
Distribution Restrictions:	~~Author Only~~	**CL/Member**	~~CL/ Member/ 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

The Center is a trademark of The Center for Medical Interoperability. All other marks are the property of their respective owners.

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 ... 6
2.3 Reference Acquisition ... 6

3 TERMS AND DEFINITIONS ... 7

4 ABBREVIATIONS AND ACRONYMS ... 8

5 OVERVIEW ... 9

6 HEALTHCARE TRUST PLATFORM (HTP) ARCHITECTURE ... 10

6.1 Trust Services ... 10
6.1.1 Registration ... 11
6.2 Trust Data Network` ... 13
6.2.1 Data Governance Policies ... 13
6.2.2 Data Transport ... 13
6.2.3 Trust Ramp ... 13
6.3 Trust Ecosystem Participants ... 13

7 CORE INTEROPERABILITY ENABLERS ... 14

7.1 Data Architecture ... 14
7.2 Provisioning and Management ... 14
7.3 Security ... 14
7.3.1 Known Identifiers ... 14
7.3.2 Secure Transport ... 14

APPENDIX I ACKNOWLEDGEMENTS ... 15

Figures

Figure 1 – Healthcare Trust Platform Document Map ... 9
Figure 2 – Healthcare Trust Platform Architecture ... 10
Figure 3 – Foundational Trust Services ... 11

Tables

Table 1: Registration Resource ... 11

1 SCOPE

1.1 Introduction and Purpose

This document specifies an initial iteration of the Healthcare Trust Platform to enhance interoperability, data liquidity, and trust among devices, systems, applications, and stakeholders in the healthcare industry. The purpose is to establish a base technical architecture and requirements to implement the Healthcare Trust Platform.

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, Jan 2018
https://medicalinteroperability.org/specifications/D02/CMI-DOC-TD-D02-2019-05-31.pdf

[C4MI-TR-HTP] "Healthcare Trust Platform Technical Architecture", Center for Medical Interoperability, Sep 2019
Document Reference: CMI-TR-HTP-WIP-06 (source: C4MI)

[C4MI-SP-HTP-IST] “HTP Identity and Security Transport”, Center for Medical Interoperability, Oct 2019
Document Reference: C4MI-TD-TP-IST-D01 (source: C4MI)

[C4MI-SP-CP] “C4MI Certificate Policy”, Center for Medical Interoperability, Oct 2019
Document Reference: C4MI-TD-TPCP-D01 (source: C4MI)

[C4MI-SP-PKI-CA] “HTP Public Key Infrastructure & Certificate Hierarchy”, Center for Medical Interoperability, Oct 2019
Document Reference: C4MI-TD-TPPCH-D01 (source: C4MI)

2.2 Informative References

This specification does not use any informative references.

2.3 Reference Acquisition

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

3 TERMS AND DEFINITIONS

This document relies on the terms and definitions specified in [CMI-DOC-TD].

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

DNS	**D**omain **N**ame **S**erver
FQDN	**F**ully **Q**ualified **D**omain **N**ame
HTP	**H**ealthcare **T**rust **P**latform
IP	**I**nternet **P**rotocol
NTP	**N**etwork **T**ime **P**rotocol
PLHR	**P**ersonal **L**ongitudinal **H**ealth **R**ecord
REST	**RE**presentational **S**tate **T**ransfer

5 OVERVIEW

The Healthcare Trust Platform (HTP) is a business and technology platform designed to enable the *creation* and *trusted exchange of value* between *ecosystem participants* (e.g., healthcare providers), and also creates and amplifies *derivative value* as direct result of these *trusted interconnections*. An overview can be found in [C4MI-TR-HTP]. This document specifies an initial iteration of this Healthcare Trust Platform.

Specifically, it considers the minimum viable set of components and interfaces to deploy an interoperable version of the Healthcare Trust Platform. Future iterations are expected to evolve this architecture further in compliance with the comprehensive platform envisioned in [C4MI-TR-HTP].

This document references and leverages the technical report and additional specifications depicted in the document map of Figure 1.

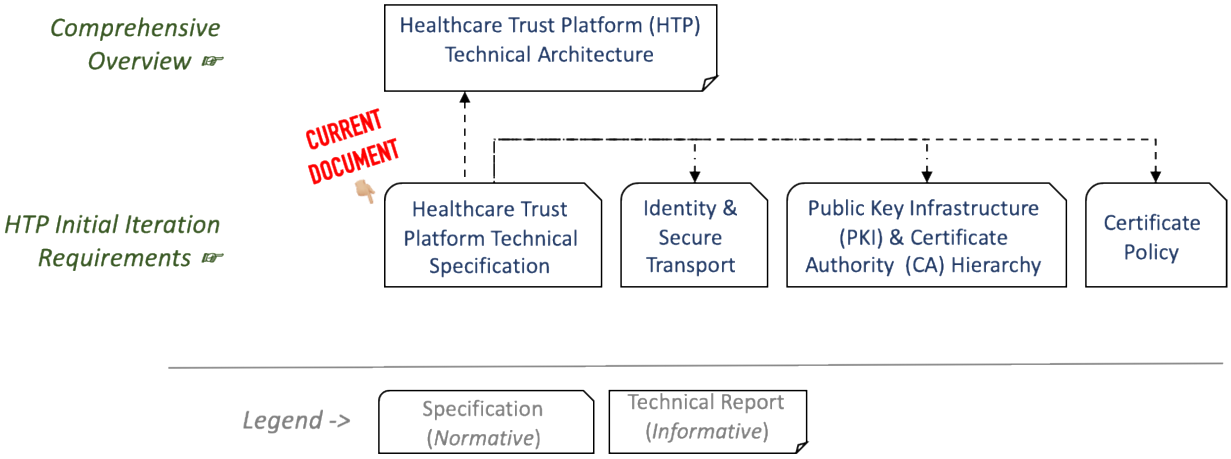
Comprehensive Overview ☞
Healthcare Trust Platform (HTP) Technical Architecture
CURRENT DOCUMENT
HTP Initial Iteration Requirements ☞
Healthcare Trust Platform Technical Specification
Identity & Secure Transport
Public Key Infrastructure (PKI) & Certificate Authority (CA) Hierarchy
Certificate Policy
Legend ->
Specification (Normative)
Technical Report (Informative)

Figure 1 – Healthcare Trust Platform Document Map

6 HEALTHCARE TRUST PLATFORM (HTP) ARCHITECTURE

The HTP consists of business and technical components. A Healthcare Trust Platform SHALL have a *Governing Authority* that ensures compliance with both.

The governing authority SHALL provide an *implementation document* indicating how the deployment instance is implemented and how trust participants can participate. The governing authority SHALL also provide the *data governance and use policies*, and any additional considerations.This governing authority SHALL also implement a *HTP technical instance* in compliance with the technical architecure this document.

The HTP technical architecture connects a set of *trust ecosystem participants* via a *trust data network* to *communicate securely;* and, offers a set of *foundational trust services* that enable participants to *register* onto the network, *discover* each other and available trust services, enforce *policy*, and provide *logging and auditing* functions for transaction verification, non-repudiation, etc. This is depicted in Figure 2.

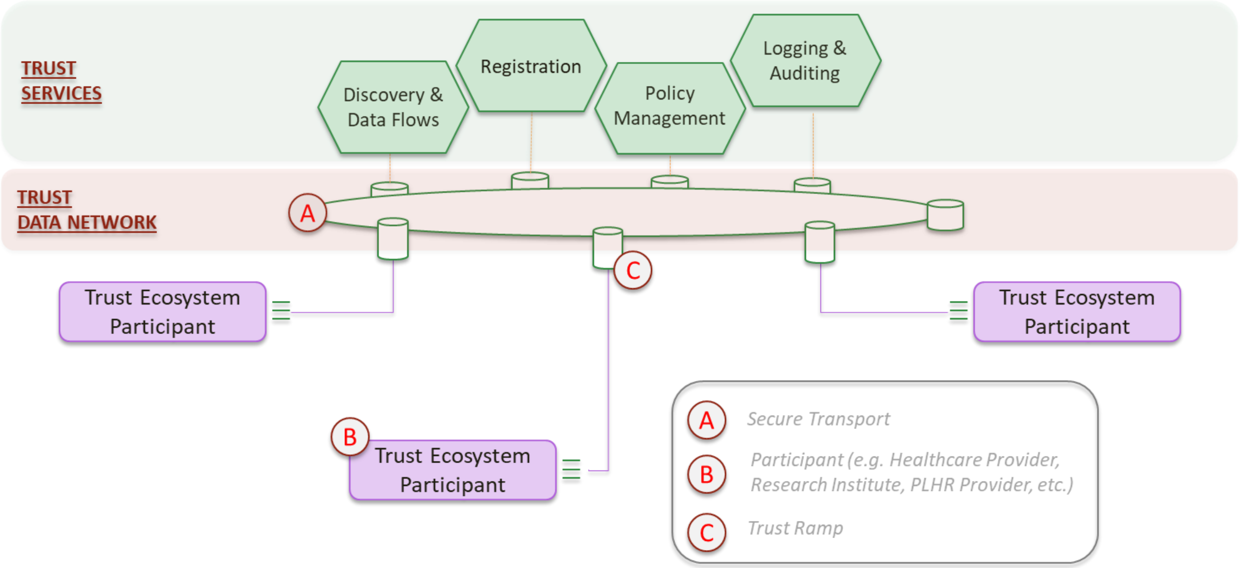
TRUST SERVICES
Discovery & Data Flows
Registration
Policy Management
Logging & Auditing
TRUST DATA NETWORK
A
C
Trust Ecosystem Participant
Trust Ecosystem Participant
B
Trust Ecosystem Participant
A Secure Transport
B Participant (e.g. Healthcare Provider, Research Institute, PLHR Provider, etc.)
C Trust Ramp

Figure 2 – Healthcare Trust Platform Architecture

This iteration of the HTP leverages these architectural concepts and specifies a compliant, base, interoperable implementation. It specifies a HTP instance where *trust participants* to connect via a *trust data network* that may be configured manually or in an automated manner. It also offers a *subset* of the *foundational trust services*. In this document the term *trust element* is generically used to refer to an *ecosystem participant or a trust service*.

6.1 Trust Services

A HTP instance that complies with this version of the document SHALL provide for the equivalent functionality of these foundational trust services: *registration, discovery and data flows, and logging and auditing*. The HTP instance SHALL also provide for *policy enforcement* to support the *data governance policies* specified by the governing authority. These are illustrated in Figure 3 , and the requirements follow.

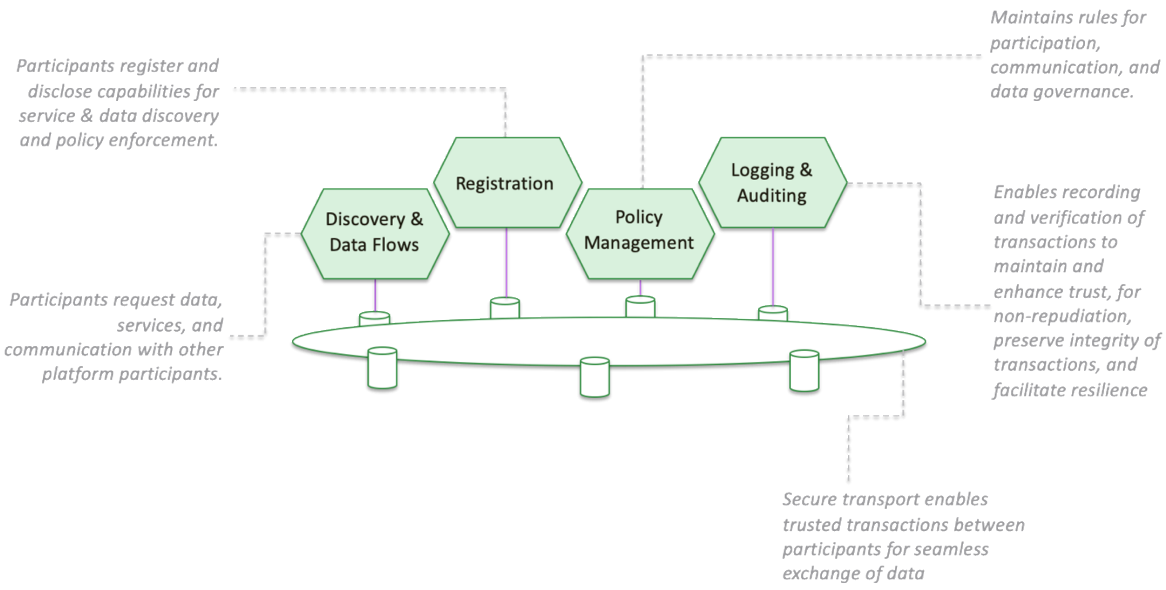
Participants register and disclose capabilities for service & data discovery and policy enforcement.
Maintains rules for participation, communication, and data governance.
Registration
Logging & Auditing
Discovery & Data Flows
Policy Management
Enables recording and verification of transactions to maintain and enhance trust, for non-repudiation, preserve integrity of transactions, and facilitate resilience
Participants request data, services, and communication with other platform participants.
Secure transport enables trusted transactions between participants for seamless exchange of data

Figure 3 – Foundational Trust Services

6.1.1 Registration

Registration service allows trust network participants and trust service elements to participate in an instance of a trust platform.

This SHALL be provided by a manually configured *registration function* or an automated *Registry* element.

An automated Registry SHALL implement the RESTful resource shown in Table 1.

Table 1: Registration Resource

Attribute	Cardinality	Description
Trust-Element-IP	0..1	*<IP address of the trust element related to this registration instance>*
Trust-Element-Type	1..n	participant | service | other where: *participant: trust ecosystem participant* *service: trust service* *other: unspecified type*
Trust-Element-Registration-Status	1..1	registration-requested | deregistration-requested | registered | deregistered | other
Trust-Element-profile	0..1	*<HTTP URL to the trust element profile; a set of capabilities that it supports that will be defined in a future effort>* *Note: the profile is not specified in this iteration, and is hence made optional.*
Trust-Element-FQDN	0..1	*<FQDN of the trust element that is provided following a successful registration; this can be used by other trust elements to reach the registered element>*
Registration-Requesting-Element-ID	0..1	*<FQDN of the trust element requesting action; included for third party actions>*
Authorization-Info	0..1	*<Authorization info; when a third-party element is performing actions on behalf of another trust element>*
Discovery-Data-Flows-Element	0..1	*<FQDN of the Discovery & Data Flows Element for use by the registered entity>*

NTP-Server	0..1	*<NTP server FQDN in case the registrant needs to synchronize at any time; provided by the registry>*
Management-Element	0..1	*<FQDN of the management element that the registrant should communicate with for management functions>*
DNS-Servers	0..n	*<IP address list of one or more DNS servers>*

The *Registration Resource* is used to perform the following functions:

6.1.1.1.1 Register

This is used to indicate willingness to participate in a trust platform instance.

When a trust element plans to participate in a HTP instance a resource creation request SHALL be presented to the Registry via the trust element directly or via another trust element on its behalf.

6.1.1.1.2 Deregister

This is used when a currently registered trust element wants to stop being part of the trust platform, e.g., because of a software update.

When a trust element plans to deregister from a HTP instance a resource update request SHALL be presented to the Registry via the trust element directly or via another trust element on its behalf. The latter is so that an authorized trust element (e.g., management) can take another trust element out of service, e.g., for cybersecurity reasons.

6.1.1.1.3 Update registration

This is used when a currently registered trust element wants to update information about itself, e.g., to modify its profile.

A trust element that wishes to update its registration SHALL send a resource update request to the registry.

6.1.1.1.4 Query registration

This is used to get information about a trust element's registration, including the registration's status, a participant's capability profile, etc.

Registry SHALL allow registration queries from authorized entities as defined by the governing entities policies.

6.1.1.2 Discovery & Data Flows

The *Discovery and Data Flows* service allow trust network participants to request data, services, and communication with other platform participants.

This iteration of the document requires this service to be based on manual configura tion.

6.1.1.3 Logging & Auditing

The *Logging & Auditing* service enables trust platform communications, management and auditing *events* to be *stored* and *verified*.

An HTP instance SHALL ensure that all transactions are logged, and the logs stored in a verifiable manner. These logs MAY be cryptographically verifiable.

6.1.1.4 Policy Management

The *Policy Management* service allows the trust platform to maintain *rules* for participation, communication, and data governance.

The governing entity of the HTP instance SHALL specify these policies.

6.2 Trust Data Network`

The trust data network is comprised of a logical set of *trust ramp* elements that proxy trust ecosystem participants for purposes of communication. The trust ecosystem participants implement *trust interfaces* to communicate with trust services and with each other.

An HTP Instance SHALL specify the *trust ramps* for its deployment. An HTP instance SHALL also specify or reference the *trust interfaces* that are allowed within the instance.

6.2.1 Data Governance Policies

The governing entity SHALL specify the data governance policies for an HTP instance.

6.2.2 Data Transport

Within an HTP instance data SHALL only be transported between trust elements that support the secure transport requirements compliant with [C4MI-SP-HTP-IST].

6.2.3 Trust Ramp

Each HTP instance SHALL specify the trust ramps that will enable trust elements to connect and participant.

6.2.3.1 Trust Metadata

This version of the HTP leaves the trust metadata requirements to the HTP implementation description.

6.3 Trust Ecosystem Participants

Each trust ecosystem participant SHALL comply with the identity requirements specified in [C4MI-SP-HTP-IST].

7 CORE INTEROPERABILITY ENABLERS

This section specifies requirements related to enablers used by this instance of the HTP.

7.1 Data Architecture

The governing authority SHALL specify any data architecture requirements to support the *trust interfaces*.

7.2 Provisioning and Management

An HTP instance SHALL use time-synchronization using NTP to ensure accuracy of transactions and transaction logs. For this version of the HTP architecture manual configuration and management of the trust elements is allowed.

7.3 Security

Security requirements include authentication, authorization, message integrity, data integrity, and privacy.

7.3.1 Known Identifiers

For an expectation of trust, each element needs to be ‘Known’. This is accomplished via identifiers and associated identities. This version of the HTP architecture SHALL use digital certificates based on the Public Key Infrastructure (PKI) and Certificate Authority (CA) specified in [C4MI-SP-PKI-CA] and in compliance with [C4MI-SP-PKI-CA].

For this version of the trust platform the following identifiers, with associated identities, are considered:

- *Known Infrastructure Trust Identifier*: the HTP instance SHALL ensure that each infrastructure element has a unique ID that can be authenticated using digital certificates.

7.3.2 Secure Transport

Within an HTP instance all trust elements SHALL comply with the secure transport requirements specified in [C4MI-SP-HTP-IST].

Appendix I Acknowledgements

This work-in-progress document is a result of internal discussions at the Center. The primary author of this document is Sumanth Channabasappa. The technical report that forms of the basis of this document is [C4MI-TR-HTP].