Healthcare Trust Platform Implementation Specification Using Cybernetica® UXP®

DRAFT

Contents

Normative References

[UXP-TECH-SPECS]	UXP Technical Specifications (2019-11-20)
[UXP-SS-INSTALL]	UXP Security Server 1.11 Installation and Configuration Guide
[UXP-SS-USER]	UXP Security Server 1.11 User Guide
[UXP-RS-INSTALL]	UXP Registry Server 1.11 Installation and Configuration Guide
[UXP-RS-USER]	UXP Registry Server 1.11 User Guide
[IETF-RFC-3161]	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[C4MI-CDUA]	C4MI Common Data Use Agreement (Draft)
[C4MI-TS-HTP]	C4MI Healthcare Trust Platform (In Progress)

Informative References

[C4MI-TR-HTP]	Healthcare Trust Platform Technical Architecture
[UXP-OVERVIEW]	UXP Technology Overview (2019-11-20)

Overview

This document specifies how to implement an instance of the C4MI Healthcare Trust Platform [C4MI-TS-HTP] leveraging the Cybernetica UXP Architecture. The Cybernetica UXP Architecture provides foundational components of the Health Trust Platform architecture, including Trust Services such as Registration and Logging & Auditing, and a Trust Data Network for secure communications between Trust Participants. For more information on Cybernetica UXP, see [UXP-OVERVIEW].

The document map in Figure 1 highlights how this document relates to others. Specifically, this document defines normative requirements for implementing the Healthcare Trust Platform Technical Architecture [C4MI-TR-HTP] by using Cybernetica UXP to meet the normative requirements defined in the Health Trust Platform Technical Specification [C4MI-TS-HTP].

This document is intended for implementers of the Health Trust Platform, Trust Participants, and associated partners. For Governing Authorities and systems architects interested in the overall platform architecture, the ‘Trust Platform Governing Authority’ section defines the overall implementation architecture and includes normative requirements on the Governing Authority for implementing the Health Trust Platform. Trust Platform Participants should look to the ‘Trust Platform Participants’ section for normative requirements relevant to platform participation.

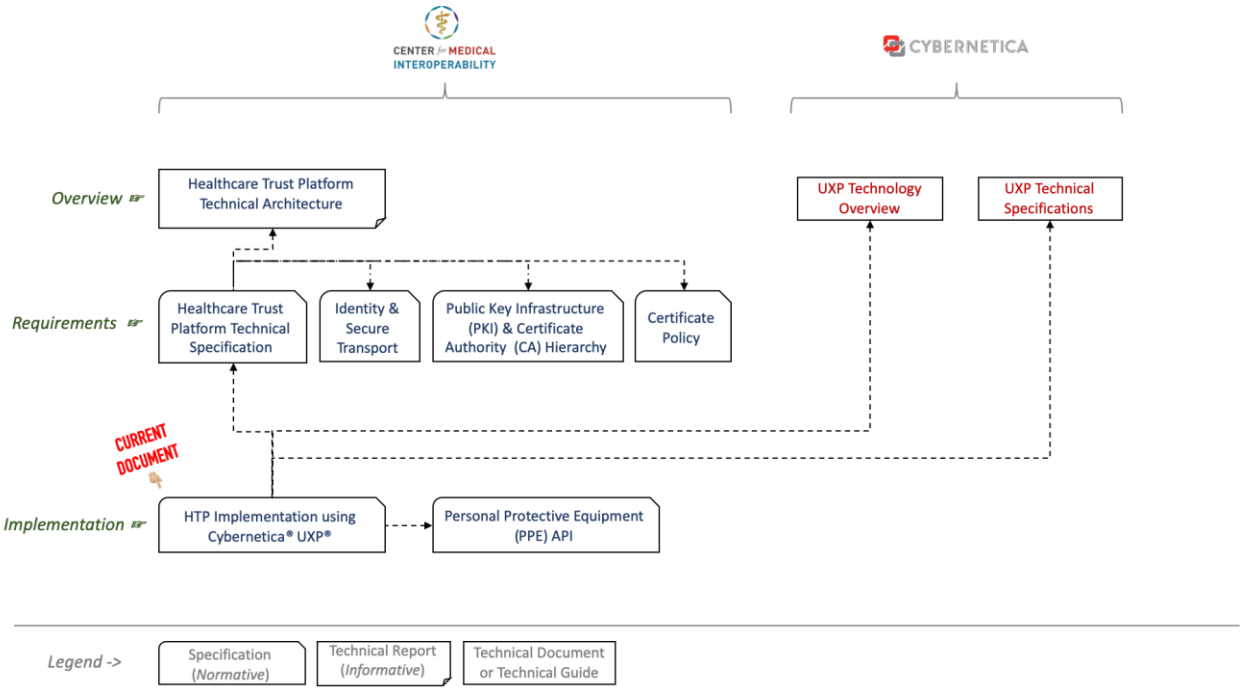

Figure 1 – Document Map

Trust Platform Governing Authority

This section specifies normative requirements related to a Governing Authority implementing the Health Trust Platform using Cybernetica UXP.

Governing Components Installation & Configuration

The Governing Authority SHALL establish a Management Services Security Server and Registry Server as described in [UXP-SS-INSTALL] and [UXP-RS-INSTALL] and operate them in accordance with [C4MI-CDUA].

The Governing Authority SHALL configure the established Registry Server as the Management Service Provider in accordance with [UXP-RS-UG], Section 4.2, as the Management Services 'Service Provider Identifier' in the Registry Server.

UXP Identifiers

The UXP Instance Identifier for the production instance of this Trust Platform is `'C4MI-HTP'`.

A UXP Member Class is a logical grouping of Trust Participants, used for a variety of purposes. UXP Member Classes are defined by C4MI. The currently defined member classes are:

- `'GA',` or equivalent – Reserved for the Governing Authority
- `'TP',` or equivalent – Reserved for Trust Participants

A UXP Member Code uniquely identifies a Participant on the Trust Platform. The UXP Member Code for the governing authority is `'GA'`. All other UXP Member Codes (e.g. for a hospital) are the organization's *Platform Organizational Identifier*, which must be applied for in accordance with [C4MI-CDUA].

A UXP Subsystem Code uniquely identifies a services or service client provided by a participant. The UXP Registry Server Subsystem Code is `'GA_mgmt'`.

The Governing Authority SHALL define the UXP Instance Identifier, Member Classes, a Member Code and Subsystem for the Governing Authority, and a Subsystem for Management Services in the Registry Server, according to the identifiers defined in this section, in accordance with [UXP-RS-USER].

Certification Services

The Governing Authority SHALL add the C4MI Root CA as the sole Approved Certification Service in the UXP Registry Server. For this Certification Service:

- The Certification Service SHALL NOT be configured to be only used for TLS authentication. (This is because certificates issued under the C4MI certificate hierarchy are used for purposes beyond authentication, such as signing for data integrity and code verification.)
- An OCSP responder SHALL NOT be defined for the Certification Service as part of the global configuration. (Responder information is instead distributed via certificates' Authority Information Access extension.)
- All Sub-CAs defined in the C4MI PKI Certificate Hierarchy SHALL be configured as Intermediate CAs.

The Governing Authority SHALL configure OCSP settings in the global configuration in accordance with [C4MI-TS-HTP].

Timestamping Services

The Governing Authority SHALL provide a Time Stamping Authority, compliant with [IETF-RFC-3161], for timestamping services for platform elements.

The Governing Authority SHALL configure the URL and certificate for the C4MI TSA in the UXP Registry Server by the Governing Authority and distributed to all Security Servers as part of the UXP global configuration.

Registration

The Governing Authority SHALL register Participants and their appropriate systems in accordance with [UXP-RS-USER] and [C4MI-CDUA].

Logging & Auditing

The Governing Authority SHALL configure logging settings in the global configuration in accordance with [UXP-RS-USER], [C4MI-RS-USER], and [C4MI-CDUA].

Trust Platform Participants

This section specifies normative requirements for Trust Platform Participants. In general, to be a Trust Platform Participant (e.g. to participate in the exchange of PPE inventory data as part of TOGETHER for PPE), an organization must be authorized and adhere to the governance policies and technical requirements defined or referenced in this section. At a high-level, a Participant must:

- Apply to be a Trust Platform Participant in accordance with [C4MI-CDUA]
- Install, configure, register, and operate UXP Security Server in accordance with this specification
- Use or provide C4MI-approved APIs in accordance with the appropriate governance policies in [C4MI-CDUA]

Security Server Installation & Configuration

A Trust Platform Participant SHALL establish and configure a Security Server in accordance with [C4MI-CDUA] and [UXP-SS-INSTALL], Sections 2 and 3, using the Configuration Anchor, UXP Member Class, and UXP Member Code obtained from the Governing Authority.

A Trust Platform Participant SHALL operate the Security Server in accordance with [C4MI-CDUA].

Certificate Configuration

A Trust Platform Participant SHALL request two digital certificates:

- ‘Trust Platform Component Authentication Certificate’
- ‘Trust Participant Signing Certificate’

These are issued by a Trust Platform Sub-CA and Trust Participant Sub-CA, respectively. These SHALL then be imported into the Security Server in accordance with [UXP-SS], Section 4.

Timestamping Service Configuration

A Trust Platform Participant SHALL add the C4MI Time Stamp Authority as a Timestamping Service according to section 3.3 of [UXP-SS-INSTALL].

Security Server Registration

A Trust Platform Participant SHALL register their 'Trust Platform Component Authentication Certificate' in accordance with [UXP-SS-INSTALL], Section 4.5, and notify the Governing Authority.

Trust Applications and Communication via REST APIs

The requirements in this section apply to any Application a Participant connects to the Trust Platform (e.g. a software system providing the PPE Inventory API).

Application Registration

A Participant SHALL define a Subsystem for their Application in accordance with [UXP-SS-USER], Section 4.2. For a C4MI-approved API, the Subsystem Code is the API's specified *Known Infrastructure Identifier* (e.g. ppe_together_inventory-1.0) as defined in [C4MI-TS-HTP].

A Participant SHALL register their Application in accordance with [UXP-SS-USER], Section 4.4, and notify the Governing Authority.

Certificate Configuration

A Trust Participant SHALL request an 'Application Certificate' be issued by an Application Provider Sub-CA.

A Trust Participant SHALL configure the communication between the Security Server Client and Security Server to be via the 'HTTPS protocol' and using the 'Verify TLS certificate' option to mutually authenticate using the Application Certificate, in accordance with Section 10 of [UXP-SS-USER].

Logging & Auditing

A Trust Participant's Application SHALL log events in accordance with [UXP-RS-USER], [C4MI-RS-USER], and [C4MI-CDUA].

Provenance and Data Integrity

When communicating via REST APIs, a Trust Participant's Application SHALL include Trust Metadata as defined in [C4MI-TS-HTP].

Operations & Maintenance

A Trust Participant SHALL operate their Applications in accordance with [C4MI-CDUA].