CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Document Together for PPE Readiness, Implementation Architecture

C4MI-TD-IA-PPE-D01-2020-08-12

Draft

Notice

This document is the result of a cooperative effort undertaken at the direction of the Center for Medical Interoperability™ (C4MI) 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 C4MI 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 C4MI. 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

DISCLAIMER

This document is furnished on an "AS IS" basis and neither C4MI 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 C4MI 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.
C4MI 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 C4MI 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 C4MI, 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

1 References 5
2 Purpose 5
3 Overview of High-Level Architecture 6
4 Component Information 7
4.1 PPE Data Export 7
4.2 PPE Import Service 7
4.3 Healthcare Trust Platform (HTP) Gateway 7
5 Deployment Information 8
5.1 Trusted Participation 8
5.1.1 Authentication and Encryption (Trusted Participation) 9
5.1.2 System Requirements (Trusted Participation) 10
5.1.3 Network Port Requirements (Trusted Participation) 10
5.2 Hosted Participation 13
5.2.1 Authentication and Encryption (Hosted Participation) 14
5.2.2 System Requirements (Hosted Participation) 14
5.2.3 Network Port Requirements (Hosted Participation) 14

Tables

Table 1. Ports required for inbound connections to PPE Import Service 10
Table 2. Ports required for outbound connections from PPE Import Service 11
Table 3. Ports required for inbound connections to HTP Gateway 11
Table 4. Ports required for outbound connections from HTP Gateway 12

Figures

Figure 1. TOGETHER for PPE Readiness Network Architecture 6
Figure 2. Network Components (Trusted Participation) 8
Figure 3. Data Flow (Trusted Participation) 9
Figure 4. Network Protocols and Ports (Trusted Participation) 10
Figure 5. Network Components (Hosted Participation) 13
Figure 6. Data Flow (Hosted Participation) 14

Document Status Sheet

Document Control Identifier:	C4MI-TD-IA-PPE
Document Title:	Together for PPE Readiness, Implementation Architecture
Revision History:	D01
Date:	08/12/2020
Status:	Draft
Distribution Restrictions:	C4MI/Member/NDA Vendor

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 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 C4MI.

1 References

[C4MI-TD-DEX-PPE] *Center for Medical Interoperability Document: TOGETHER for PPE Readiness, Data Export,* C4MI-TD-DEX-PPE-D06-2020-04-15
Available: https://medicalinteroperability.org/specifications/

[C4MI-TD-TPPCH] Center for Medical Interoperability Document: Trust Platform PKI Certificate Hierarchy, C4MI-TD-TPPCH-D06-2020-03-30
Available: https://medicalinteroperability.org/specifications/

[IETF-RFC5246] *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC5246, August 2008.
Available: https://tools.ietf.org/html/rfc5246

2 Purpose

This document presents the architecture, network, security and authorization considerations for trust participants (e.g., health systems, hospitals) to participate in the TOGETHER for PPE Readiness project to share PPE data via the C4MI Healthcare Trust Platform (HTP).

3 Overview of High-Level Architecture

Participating organizations include one or more hospitals and one or more Inventory Systems that contain data about the represented hospitals' PPE inventory. The Inventory System(s), or their administrators, export inventory updates as a CSV data export file which is transferred by SFTP or other secure means to the PPE Import Service. The PPE Import Service imports the data and transmits it via a HTP Gateway to the PPE Data Services.

The PPE Data Services include a PPE Data Cache and PPE Product Catalog. Data sent to the PPE Data Services element is stored in the PPE Data Cache, which provides PPE FHIR API endpoints for access to blinded and unblinded data. Future PPE data visualization or analytics applications can utilize this set of PPE FHIR APIs for access to the PPE data (blinded or unblinded as authorized). The PPE Product Catalog (maintained and curated by C4MI) is a source of truth for PPE product data. PPE Data Services normalize participant-reported products against the catalog, and queues up new reported products or reported products needing review for C4MI to analyze and reconcile. The curation of this catalog is done through an administrative API provided by the PPE Data Services element. (An analogous site catalog, API, and curation process is also in place as a source of truth for information about reporting hospitals.) PPE Data Services are hosted by C4MI.

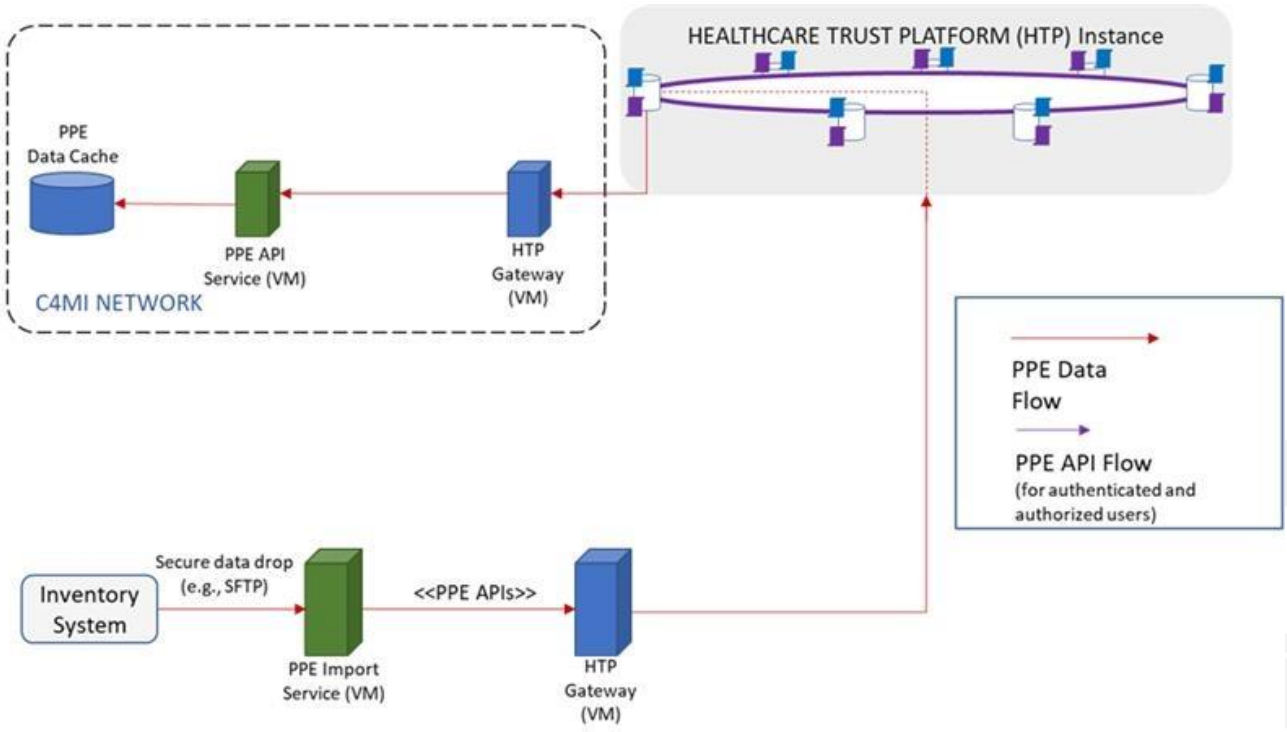

Figure 1. TOGETHER for PPE Readiness Network Architecture

4 Component Information

The *PPE Import Service* collects the *PPE data export* from the inventory systems as a CSV file, and transmits it via the HTP Gateway to the HTP instance associated with the TOGETHER for PPE effort. The *HTP Gateway* enables trusted exchange of the PPE data across a mutually authenticated channel with the HTP instance associated with the TOGETHER for PPE effort. To facilitate this it contains a Cybernetica® UXP® application on an Ubuntu® Linux® operating system.

4.1 PPE Data Export

Participants are responsible for establishing a daily PPE data export, which includes daily PPE inventory and order data for each of the participant's hospitals. See [C4MI-TD-DEX-PPE] for detailed requirements.

4.2 PPE Import Service

The PPE Import Service consumes the data export file(s) and acts as a client to the PPE Data Services element, sending inventory data using FHIR REST APIs via the HTP Gateway for proxied communication. The Import Service watches a specific directory for export files; participants may transfer the export files to that directory securely, e.g., via SFTP.

4.3 Healthcare Trust Platform (HTP) Gateway

The Healthcare Trust Platform Gateway proxies communication between applications and services deployed on the Healthcare Trust Platform. It provides a mechanism for identifying participants, distributing configurations, deploying service-level authorization policies, and providing provable transaction logging for auditing purposes.

5 Deployment Information

There are two deployment models for these components.

- **Trusted Participation:** where the participant hosts components required to connect to the HTP Trust Platform. In this case, participants are expected to host, secure, and configure (e.g., with digital certificates) certain elements within their network to ensure trusted communications.
- **Hosted Participation:** where C4MI hosts the trust components on behalf of a trust participant who channels data via the hosted trust infrastructure. This form of participation is transitionary, with the intended end-goal of Trusted Participation.

The following section describes technical deployment details for both models. (In both cases, participants first sign applicable business and legal agreements.)

5.1 Trusted Participation

This section describes requirements for "Trusted Participation" deployments. Diagrams in this section illustrate the network components that will be deployed by C4MI and the participant networks (Figure 2), data flow (Figure 3) and the network protocols in use within the participant network (Figure 4).

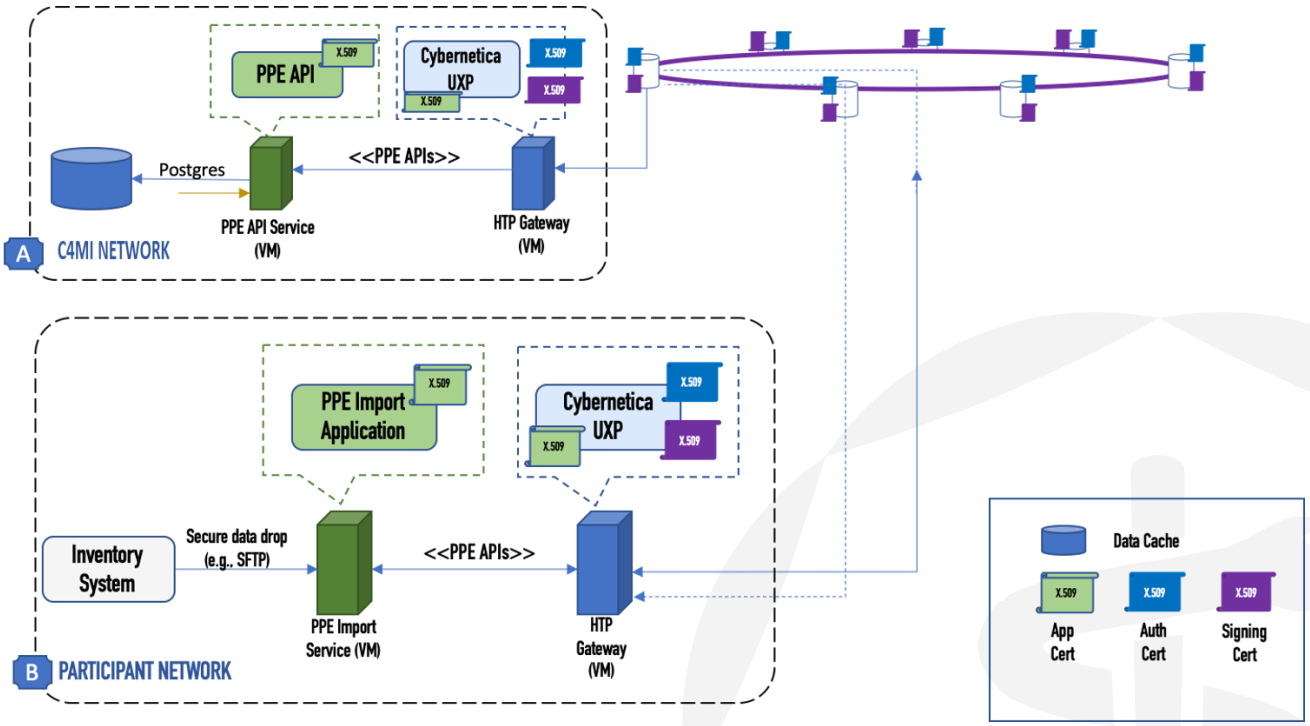

Figure 2. Network Components (Trusted Participation)

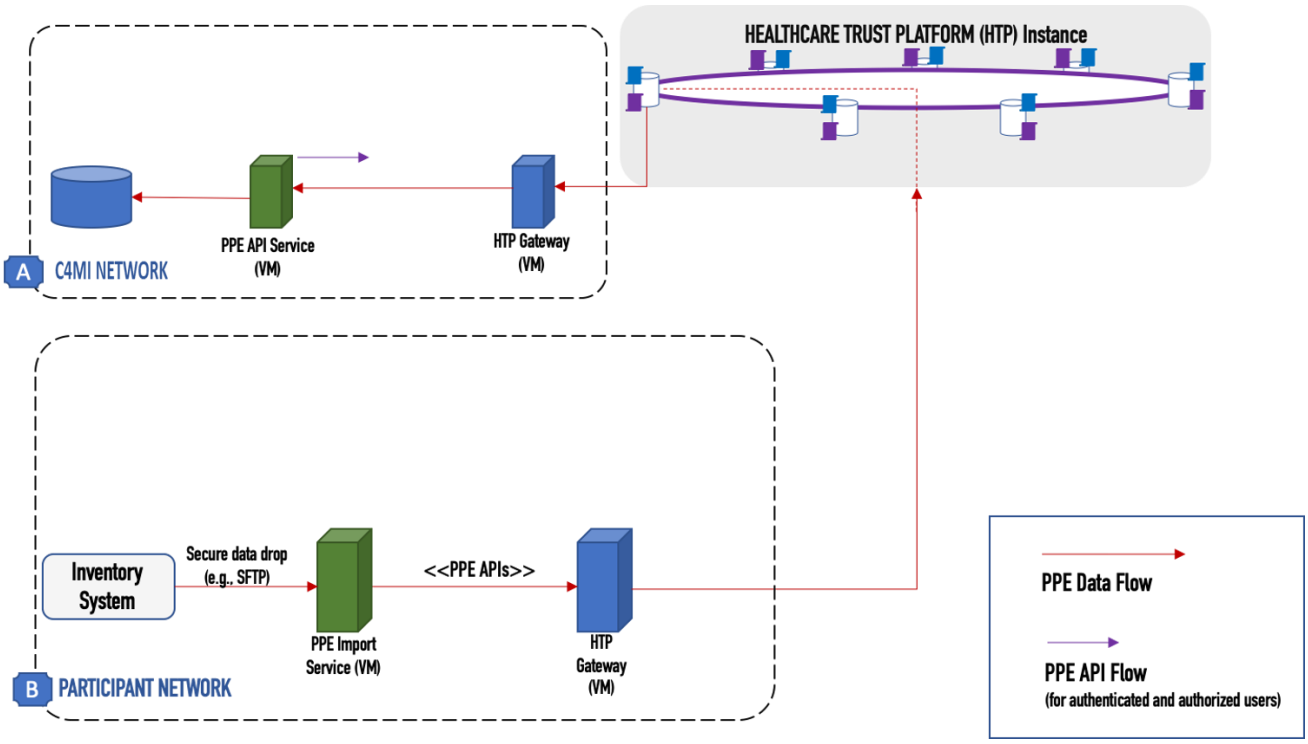

Figure 3. Data Flow (Trusted Participation)

5.1.1 Authentication and Encryption (Trusted Participation)

Export files are transmitted to the watched directory on the PPE Import Service from inventory systems using a participant's standard operating procedures for securely transferring files, e.g., via SFTP.

The PPE Import Service and the Cybernetica UXP applications are configured with X.509 digital certificates to enable mutual authentication and encryption prior to communications using TLS 1.2 ([IETF-RFC5246]). These certificates are issued as part of the C4MI PKI Infrastructure and its certificate hierarchy ([C4MI-TD-TPPCH]).

The PPE Import Service has one application digital certificate. This is used for mutually authenticated communications over TLS 1.2 with the HTP Gateway.

The HTP Gateway has three digital certificates: *Trust Platform Component Authentication Certificate*, the *Trust Participant Signing Certificate*, and the *Application Certificate*. The T*rust Platform Component Authentication Certificate* is used for secure communications. The *Trust Participant Signing Certificate* is used to provide data integrity. The *Application Certificate* is used to secure connections to clients, including the PPE Import Service.
Participants are responsible for configuring and maintaining the connection between the PPE Import Service and HTP Gateway, which will be secured via TLS 1.2 and mutually authenticated using C4MI-issued Application Certificates. Participants are also responsible for maintaining the integrity of any certificates issued to the Participant from the C4MI PKI.

5.1.2 System Requirements (Trusted Participation)

The PPE Import Service and HTP Gateway may be deployed either on premises or in a cloud environment such as Amazon Web Services (AWS) or Microsoft Azure.
The PPE Import Service is to be deployed in an Ubuntu 18.04 virtual machine. Minimum requirements for the VM are a 64-bit dual-core Intel, AMD or compatible CPU, 1 GB RAM, a 100 Mbps network interface card, and 20GB disk space.
The HTP Gateway is to be deployed in an Ubuntu 18.04 virtual machine. Minimum requirements for the VM are a 64-bit dual-core Intel, AMD or compatible CPU (AES instruction set support is highly recommended), 3 GB RAM, and a 100 Mbps network interface card. Disk space requirements will be communicated during the onboarding process to account for data volume variation between participants.

5.1.3 Network Port Requirements (Trusted Participation)

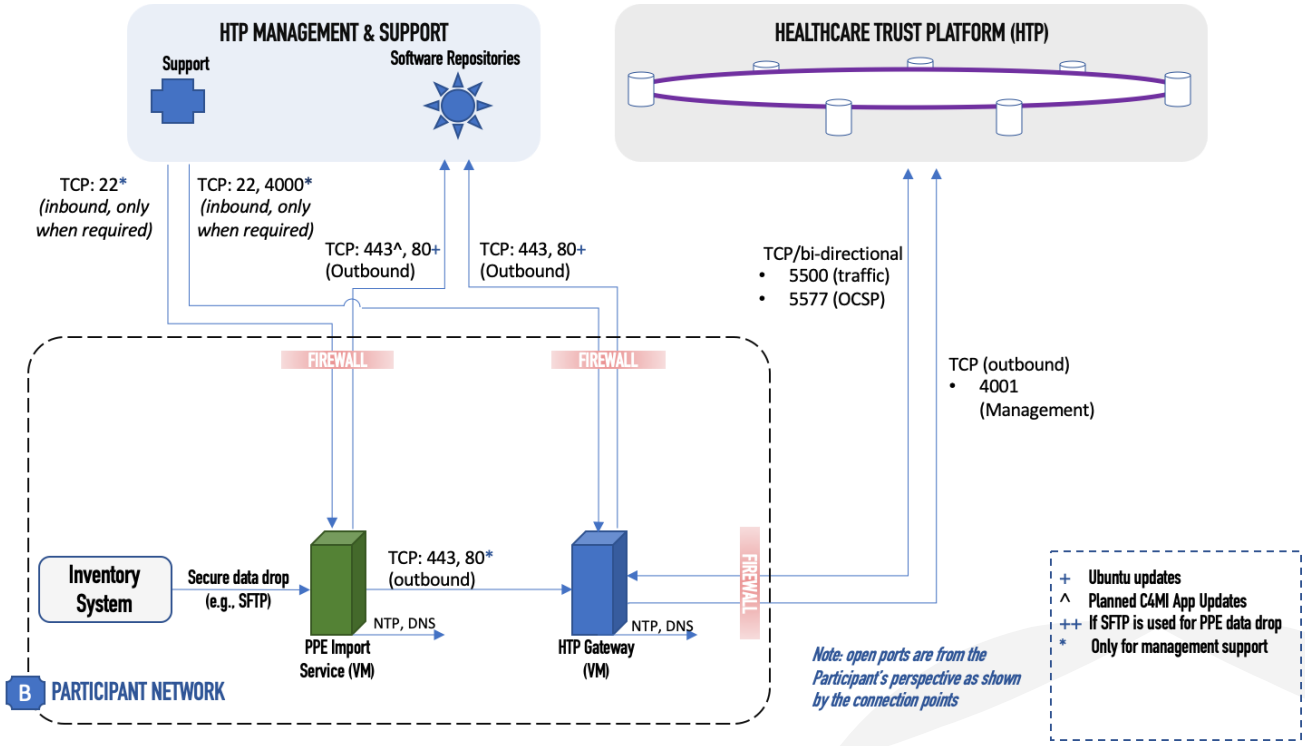

Figure 4. Network Protocols and Ports (Trusted Participation)

Table 1. Ports required for inbound connections to PPE Import Service

Port (TCP)	Purpose	Network scope
22	SFTP access for export file transfer	PRIVATE
22	SSH access	PRIVATE (Mgmt & Support)

Table 2. Ports required for outbound connections from PPE Import Service

Port (TCP)	Purpose	Network scope
80	HTTP connections to HTP Gateway	PRIVATE
443	HTTPS connections to HTP Gateway	PRIVATE
80	Software updates	PUBLIC
443	Software updates	PUBLIC
Port (UDP)	**Purpose**	**Network scope**
53	DNS	PUBLIC
123	NTP	PUBLIC

Table 3. Ports required for inbound connections to HTP Gateway

Port (TCP)	Purpose	Network scope
22	SSH access	PRIVATE (Mgmt & Support)
4000	Access to the web-based user interface	PRIVATE (Mgmt & Support)
80	HTTP connections from applications	PRIVATE
443	HTTPS connections from applications	PRIVATE
5500	UXP message exchange between UXP Security Servers	PUBLIC
5577	Querying OCSP responses between UXP Security Servers	PUBLIC

Table 4. Ports required for outbound connections from HTP Gateway

Port (TCP)	**Purpose**	**Network scope**
80	HTTP connections to applications	PRIVATE
443	HTTPS connections to applications	PRIVATE
5500	Message exchange between UXP Security Servers	PUBLIC
5577	Querying OCSP responses between UXP Security Servers	PUBLIC
4001	Query global configuration from Registry Server (HTTPS)	PUBLIC
80	Software updates	PUBLIC
443	Software updates	PUBLIC
Port (UDP)	**Purpose**	**Network scope**
53	DNS	PUBLIC
123	NTP	PUBLIC

5.2 Hosted Participation

This section describes requirements for "Hosted Participation" deployments. Diagrams in this section illustrate the network components that will be deployed by C4MI and the participant networks (Figure 5) and Data Flow (Figure 6).

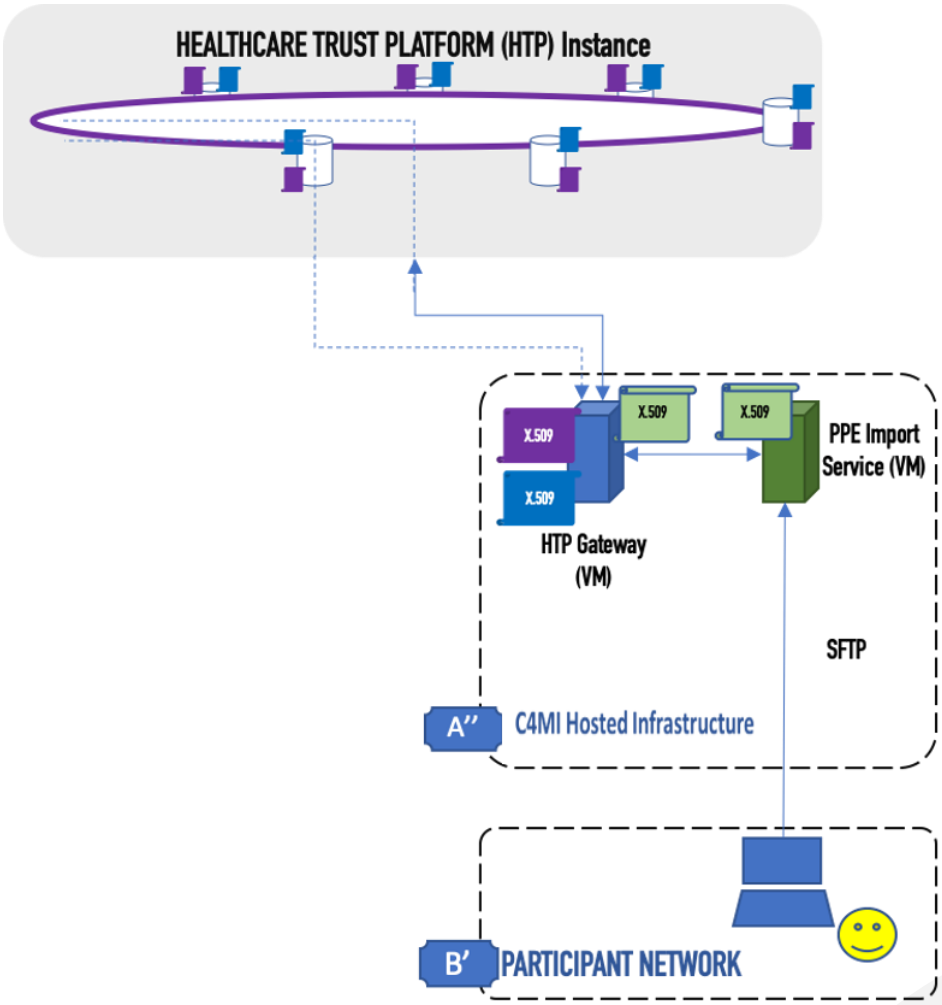

Figure 5. Network Components (Hosted Participation)

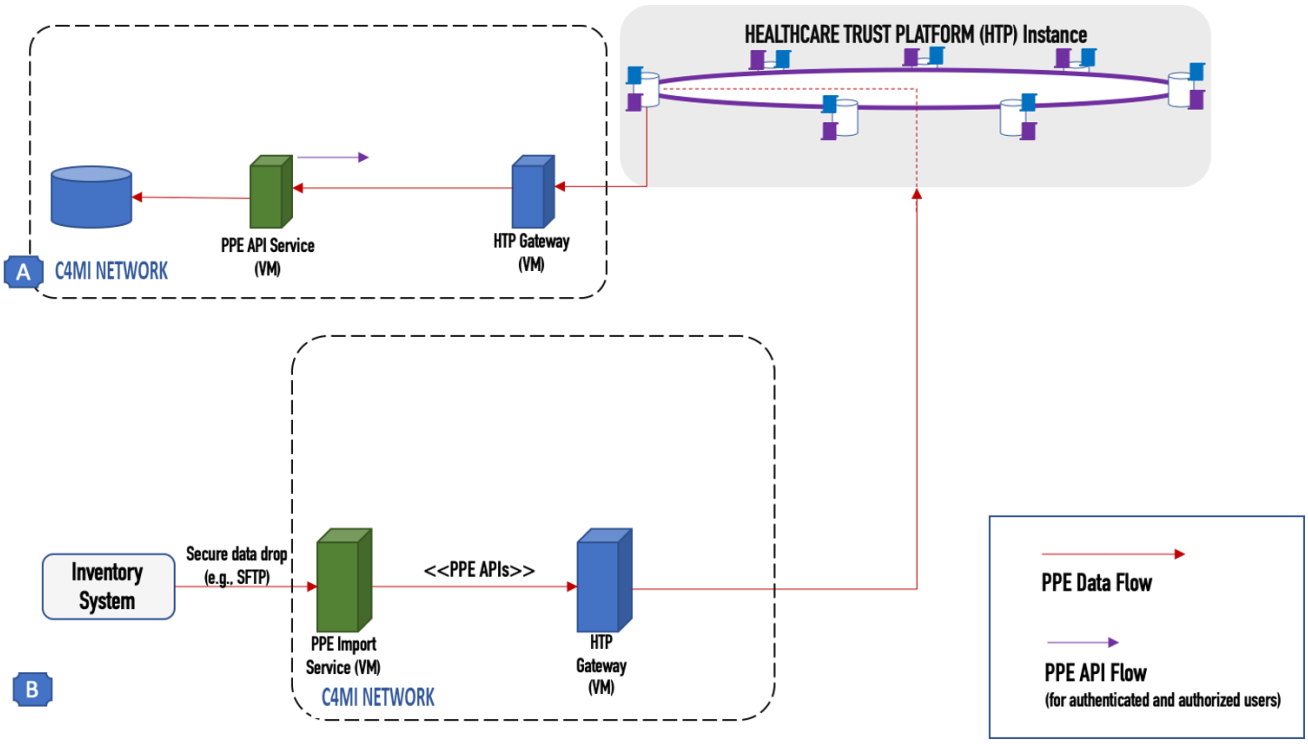

Figure 6. Data Flow (Hosted Participation)

5.2.1 Authentication and Encryption (Hosted Participation)

A participant shares a Secure Shell (SSH) public key for C4MI to setup SFTP access and uses SFTP to upload data files from its inventory system to a C4MI host server. Participants are responsible for maintaining the integrity of the private key associated with the shared public key. All authentication and encryption requirements inside the hosted network are the responsibility of C4MI.

5.2.2 System Requirements (Hosted Participation)

Participant does not maintain any system components in the "Hosted Participation" deployment.

5.2.3 Network Port Requirements (Hosted Participation)

Participant must configure their network to support sending data exports via SFTP to C4MI.