Integrating the Healthcare Enterprise

IT Infrastructure (ITI)
White Paper

Survey of Network Interfaces Form

Revision 1.1 – Published

Date: May 29, 2020

Author: IHE ITI Technical Committee

Email: iti@ihe.net

Please verify you have the most recent version of this document. See here for Published Versions and here for Public Comment versions.

Foreword

This is a white paper of the IHE IT Infrastructure (ITI) domain.

This white paper is published on May 29, 2020. Comments are invited at any time and can be submitted http://www.ihe.net/ITI_Public_Comments.

General information about IHE can be found at http://ihe.net.

Information about the IHE IT Infrastructure domain can be found at http://ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE IT Infrastructure Technical Framework can be found at http://ihe.net/Technical_Frameworks.

CONTENTS

1 Introduction

This IHE IT Infrastructure Survey of Network Interfaces Form (SNIF) White Paper describes the need for, the value of, and the approach for establishing a central data source of technical connectivity details for HL7®[1] v2, XD*, DICOM®[2] and FHIR®[3] endpoints to support search and retrieval of services and endpoints.

1.1 Purpose of the Survey of Network Interfaces Form White Paper

During system implementation within a healthcare institution, identification of endpoint service connection details requires the cooperation of the healthcare institution, integrators and vendors. Once a system is deployed into clinical use, these details are often difficult to find due to dispersal of the project team, inadequate record keeping, and configuration changes. The proposal of this white paper is to start with a standardized form.

The purpose of this white paper is to present the issues within the healthcare enterprise relating to the cataloguing, search and retrieval of endpoint service connection details, describes related use cases and proposes a minimally viable IHE profile to address desirable situation use cases in Section 3.2.2 below.

1.2 Scope

This white paper encompasses the cataloguing, search and retrieval of endpoint connectivity details for standards commonly profiled within IHE. Although SNIF could be useful in documenting intra-system interfaces not exposed to the enterprise, (such as failover or load balancing), and in implementing and managing security controls, these use cases are out of scope for this white paper.

1.3 Intended Audience

The intended audience of the IHE ITI Survey of Network Interfaces Form White Paper is:

- IT departments of healthcare institutions
- Integrators, consultants and interface analysts
- Technical staff of vendors participating in the deployment and service of healthcare applications

[1] HL7 is the registered trademark of Health Level Seven International and the use does not constitute endorsement by HL7.
[2] DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.
[3] FHIR is the registered trademark of Health Level Seven International and the use does not constitute endorsement by HL7.

1.4 Open Issues and Questions

Open Issue 1:

What level of portability, availability and openness should be proposed to access SNIF (such as discovery of the repository, access to, and searching within the repository)? We recognize a trade-off between accessibility/convenience and exposure of network connectivity details with access to PHI.

Open Issue 1 response:

There are two aspects to security:

1. what elements should be included within the form (Open Issue 4) and,
2. what security controls are required to access the form itself (this Open Issue). An initial proposal suggests that ATNA could be leveraged a dependency for both issues is included within the profile.

Public comment is sought on this approach, as well as additional security control baselines that should apply to a SNIF data source based on requirements and guidelines such as: NIST 800-53[4], MDR 2017/745[5], EU Directive on Security of Network and Information Systems[6], EU GDPR[7], EU Cybersecurity Act[8], ANSI/NEMA HN 1-2019[9], ISO/IEC 27001/2 and FIPS 140-3 for US Federal Agencies[10].

Open Issue 2:

What amount of security information should be included within the data model without compromising security?

Consider, although not intended as a security tool, SNIF could aid in aid in a project to map an existing network[11].

Open Issue 2 response:

An initial proposal suggests that ATNA options could be included within the data model.

Public comment is sought on this approach, as well as additional data elements such as:

- security risk assessment level and/or classification,
- link to a MDS2,
- VLAN details (e.g., encrypted VLAN used to secure legacy equipment),

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf#page=51
5 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745
6 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148
7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
8 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881
[9] https://www.nema.org/Standards/Pages/manufacturer-disclosure-statement-for-medical-device-security.aspx?key=67ri900e6rt5af#download
[10] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
[11] https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/networks/manageable-network-plan.cfm

- CA authority, public key, TLS version and authentication token.

Note: these may duplicate information in an existing security management database.

Open Issue 3:

How should the data be organized? Should there be 1 form per system or 1 form per site?

Open Issue 3 response:

The form is a virtual form and should allow for one or more; public comment is sought on this approach.

Open Issue 4:

Are the assumptions regarding an institution's role in interface management correct? Initial feedback suggests that institutions tend not to catalogue endpoints, however there is some interest in having such information available, in order to become more self-sufficient.

Open Issue 4 response:

Seek public comment on the following:

- Are interface endpoints catalogued today? If so, who maintains the catalogue?
- If an endpoint catalogue was standardized, would institutions and vendors adopt it?
- Would institutions be willing to transition their current systems to one that is standardized?

Open Issue 7:

Regarding a SNIF Profile:

- Is there a preferred technical approach based on existing standards, referenced in Section 2.2 below?
- Is there any interest from an organization willing to develop an opensource implementation as a project related to the SNIF profiling activity?
- Should SNIF have focus on implementation and break-fix use cases, or should it take a greater role in routine network transactions (i.e., reference SNIF in lieu of a static host file)?
- SNIF-like functionality is exercised in the Carequality/eHealth Exchange Provider Directory, what Carequality attributes should be included in SNIF (and vice-versa)?

Open Issue 8:

SNIF Repositories:

- How should multiple SNIF Repositories be managed? Is there a need for an authoritative Repository and defined data management policies? Do Digital Signatures offer a solution? Should only one SNIF Repository be allowed (as with an XDS Registry)? See Sections 4.1and 4.4.3 below.

- Should the Repository query Content Creators for updates or does this add unnecessary complexity (i.e., should bi-directional transactions be established as discussed in Section 4.4.2 below)?

Open Issue 9:

To what extent should connectivity details be incorporated in the data model to differentiate an endpoint without being overly exhaustive? Noting that the more information that is included, the more of a burden SNIF can be to maintain. Public comment is sought on:

- The data element "Period" was borrowed from the FHIR Endpoint resource. There are several other timestamps that could be included such as: created in repository, last updated in repository, created by content creator, last updated by content creator. This could reach a tipping point and lend towards recording such information in an audit trail. What is the preferred approach for timestamps?
- Which fields are suited for encoding as identifiers for machine readability?
- Are there recommended standards that can satisfy one or more groups of the data model (Administrative, Operational or Technical)? Is there a better grouping that enables use of existing standards?
- How should the data model handle synchronous vs. asynchronous services?

Open Issue 10:

How can this profile avoid interfering with facility network inventory/configuration management systems? Some facilities already maintain system-wide configuration inventories that identify all network connected systems, their addresses, identification, etc. These typically do not capture vendor specific or standards-based interoperability protocol configurations; they manage network addresses, ports, make/model, responsible party, etc.

Other facilities will be establishing such systems because this kind of network management is a basic starting point for all security management frameworks.

Initial feedback suggests that facilities manage the network layer, not the application layer, however, further comment is sought on two potential points of interference:

- Use of SNIF creates information inconsistency between the facility system and the SNIF system. This is usually the result of updating one but not the other system.
- SNIF system could be mis-used as a substitute for a facility system.

1.5 Closed Issues

Closed Issue 1:

Is there incentive for the healthcare institution to own and manage configuration details? Such details are typically held by vendors and within vendor systems.

Data can quickly become obsolete through movement within the facility, upgrades or de-installations; further de-incentivizing institutions to maintain this information. What model should be used for data collection? Manual entry is not sustainable.

Closed Issue 1 response:

To reduce, and possibly eliminate the need for healthcare institutions to create and maintain configuration details, a vendor supported, shared model is proposed in 4.1 below. This proposes a model in which connectivity details held within vendor applications are exposed in a standardized manner. By reducing the resources required to manually maintain SNIF, we are hoping to incentivize adoption.

Closed Issue 2:

Should the profile include provisions for automated or self-configuration (e.g., automated XCA-I config, or fully automated Connectathon setup)?

Closed Issue 2 response:

An interpretation of automated and self-configuration may be found in Section 4.7 below. The initial scope of this profile is to establish common content, and a means to access content pertaining to technical configuration details. Future extensions could include discovery and automation upon successful adoption of the initial profile.

2 Summary

The search for and discovery of system-to-system interface connection details enabling IHE profiles within the healthcare enterprise can be burdensome throughout the application lifecycle of installation, upgrade and repair.

2.1 Problem Description

Interfaces are often manually configured, requiring trained integrators to gather configuration properties, configure and test interoperability. The human element introduces the opportunity for errors, often typographical, that can be difficult to identify and correct. The increasing adoption of secure connectivity protocols complicates connectivity by introducing additional connectivity properties, such as logging, and certificates.

There are no public figures on the specific price for the configuration of interoperable products, however there is much commentary on the expense associated with system integration, upgrade and repair. One paper estimates a savings of seven hours when a configuration management tool is used to assist in the set up a new cath lab[12].

The participation and role of institutions in the management of endpoints varies. The level of interface endpoint cataloguing ranges from not at all to incomplete and informal. Catalogues that are established may be maintained by the institution, consultants, vendors or a combination of any of the three.

During the implementation of a new system, some institutions can readily provide endpoint interfaces; most do not maintain a catalogue, taking days or weeks to compile a site inventory.

[12] https://www.ijert.org/research/dicom-configuration-management-using-configuration-cockpit-tool-IJERTCONV6IS13190.pdf

Standards, documentation, and endpoint capabilities are not maintained by or known to institution IT staff. Endpoint interface details are often siloed within each systems' administrative interfaces.

Process barriers include limited institutional resources, restricted access to vendor-maintained configurations, inconsistent user interfaces for accessing system configurations, incomplete system inventories across the institution, and unknown connectivity properties, features and requirements.

Technical barriers include the lack of a standard set of metadata defined for healthcare system interfaces, and the lack of an API to search and retrieve this information for each interface.

2.2 System Configuration Catalogs in Other Work Items

The challenge of configuration registration and discovery is not unique to interoperability associated with IHE profiles, a non-exhaustive list of configuration solutions and standards may be found below, none of which are widely adopted in healthcare.

2.2.1 IHE

2.2.1.1 Connectathon Testbed

During an IHE Connectathon, technical details of hundreds of endpoints must be catalogued, searched and retrieved in order to perform peer to peer interoperability connectivity testing. A searchable configuration data source for web services, DICOM and HL7 v2[13] within the Gazelle Test Management system allows test participants to create, update, view and .csv export endpoint details.

[13] https://gazelle.ihe.net/content/system-configuration

Sys	Table	Type	Actor	Host name	IP	Port	is Secured ?	Details 1	Details 2
OTHER_IHEUSA_PATIENT_MGR_2020 / IHEUSA	None	HL7 V2 Initiator	ADT - ADT Patient Registration	gazelle-tools	10.242.128.42		false	OTHER_IHEUSA_PATIENT / IHEUSA	
OTHER_IHEUSA_GSS_2020 / IHEUSA	None	Syslog	ARR - Audit Record Repository	iheusa48	10.242.128.208	514	false	UDP	
OTHER_IHEUSA_GSS_2020 / IHEUSA	None	Syslog	ARR - Audit Record Repository	iheusa48	10.242.128.208	80	false	TCP	
OTHER_IHEUSA_GSS_2020 / IHEUSA	None	Syslog	ARR - Audit Record Repository	iheusa48	10.242.128.208	1024	true	TCP	
OTHER_IHEUSA_XDS_Toolkit_2020 / IHEUSA	K29	HL7 V2 Responder	DOC_REGISTRY - Document Registry	xds-tools	10.242.128.48	4043	false	OTHER_IHEUSA_XDSTool / IHEUSA	
OTHER_IHEUSA_XDS_Toolkit_2020 / IHEUSA	K29	Webservice	DOC_REGISTRY - Document Registry	xds-tools	10.242.128.48	80	false	ITI-18:Stored Query:sq.b	http://xds-tools/your_url
OTHER_IHEUSA_XDS_Toolkit_2020 / IHEUSA	K29	Webservice	DOC_REGISTRY - Document Registry	xds-tools	10.242.128.48	80	false	ITI-42:Register.b:r.b	http://xds-tools/your_url
PACS_IHEUSA_DICOM_ARCHIVE_2020 / IHEUSA	None	Dicom SCU	IM - Image Manager/Archive	central-archive	10.242.128.43		false	DCM4CHEE	
PACS_IHEUSA_DICOM_ARCHIVE_2020 / IHEUSA	None	Dicom SCP	IM - Image Manager/Archive	central-archive	10.242.128.43	2017	false	PACS_IHEUSA_DICO	
PACS_IHEUSA_DICOM_ARCHIVE_2020 / IHEUSA	None	Dicom SCU	IM - Image Manager/Archive	central-archive	10.242.128.43		false	PACS_IHEUSA_DICO	
PACS_IHEUSA_DICOM_ARCHIVE_2020 / IHEUSA	None	HL7 V2 Responder	IM - Image Manager/Archive	central-archive	10.242.128.43	4017	false	PACS_IHEUSA_DICOM_AR / IHEUSA	
PACS_IHEUSA_DICOM_ARCHIVE_2020 / IHEUSA	None	Dicom SCP	IM - Image Manager/Archive	central-archive	10.242.128.43	11112	false	DCM4CHEE	
PACS_IHEUSA_DICOM_ARCHIVE_2020 / IHEUSA	None	Webservice	IMG_DOC_RESPONDER - Imaging Document Responder	central-archive	10.242.128.43	80	false	RAD-129:QIDO-RS Query	http://central-archive/your_url
PACS_IHEUSA_DICOM_ARCHIVE_2020 / IHEUSA	None	Webservice	IMG_DOC_SOURCE - Imaging Document Source	central-archive	10.242.128.43	80	false	RAD-107:WADO-RS Retrieve	http://central-archive/your_url
OTHER_IHEUSA_XDS-I_2020 / IHEUSA	None	Dicom SCP	IMG_DOC_SOURCE - Imaging Document Source	xds-imaging-tools	10.242.128.209	2017	false	OTHER_IHEUSA_XDS	
OTHER_IHEUSA_XDS-I_2020 / IHEUSA	None	Dicom SCP	IMG_DOC_SOURCE - Imaging Document Source	xds-imaging-tools	10.242.128.209	2762	true	OTHER_IHEUSA_XDS	
OTHER_IHEUSA_XDS-I_2020 / IHEUSA	None	Dicom SCU	IMG_DOC_SOURCE - Imaging Document Source	xds-imaging-tools	10.242.128.209		false	OTHER_IHEUSA_XDS	
OTHER_IHEUSA_XDS-I_2020 / IHEUSA	None	Webservice	IMG_DOC_SOURCE - Imaging Document Source	xds-imaging-tools	10.242.128.209	80	false	RAD-55:WADO Retrieve	http://xds-imaging-tools/your_url
OTHER_IHEUSA_XDS-I_2020 / IHEUSA	None	Webservice	IMG_DOC_SOURCE - Imaging Document Source	xds-imaging-tools	10.242.128.209	8080	true	RAD-55:WADO Retrieve	https://xds-imaging-tools:8080/your_url
OTHER_IHEUSA_XDS-I_2020 / IHEUSA	None	Webservice	IMG_DOC_SOURCE - Imaging Document Source	xds-imaging-tools	10.242.128.209	80	false	RAD-69:Retrieve Imaging Doc Set	http://xds-imaging-tools/your_url
OTHER_IHEUSA_XDS-I_2020 / IHEUSA	None	Webservice	IMG_DOC_SOURCE - Imaging Document Source	xds-imaging-tools	10.242.128.209	8080	true	RAD-69:Retrieve Imaging Doc Set	https://xds-imaging-tools:8080/your_url
OTHER_IHEUSA_ORDER_MANAGER_2020 / IHEUSA	None	HL7 V2 Initiator	OF - Department System Scheduler/Order Filler	gazelle-tools	10.242.128.42		false	OTHER_IHEUSA_ORDER_M / IHEUSA	
OTHER_IHEUSA_ORDER_MANAGER_2020 / IHEUSA	None	Dicom SCP	OF - Department System Scheduler/Order Filler	gazelle-tools	10.242.128.42	10003	false	RAD_OF	
OTHER_IHEUSA_ORDER_MANAGER_2020 / IHEUSA	None	HL7 V2 Responder	OF - Department System Scheduler/Order Filler	gazelle-tools	10.242.128.42	10105	false	OM_RAD_OF / IHE	
OTHER_IHEUSA_ORDER_MANAGER_2020 / IHEUSA	None	HL7 V2 Initiator	OP - Order Placer	gazelle-tools	10.242.128.42		false	OTHER_IHEUSA_ORDER_M / IHEUSA	
OTHER_IHEUSA_ORDER_MANAGER_2020 / IHEUSA	None	HL7 V2 Responder	OP - Order Placer	gazelle-tools	10.242.128.42	10104	false	OM_RAD_OP / IHE	
OTHER_IHEUSA_PATIENT_MGR_2020 / IHEUSA	None	HL7 V2 Initiator	PDS - Patient Demographics Supplier	gazelle-tools	10.242.128.42		false	OTHER_IHEUSA_PATIENT / IHEUSA	
OTHER_IHEUSA_ORDER_MANAGER_2020 / IHEUSA	None	HL7 V2 Initiator	PDS - Patient Demographics Supplier	gazelle-tools	10.242.128.42		false	OTHER_IHEUSA_ORDER_M / IHEUSA	

Figure 2.2.1.1-1: Sample IHE Connectathon Configurations in Gazelle Test Management

2.2.1.2 IHE PCD Domain Configuration Use Cases

The IHE Patient Care Device (PCD) Domain concentrates on profiles pertaining to patient-centric point-of-care medical devices (such as vital signs monitors and infusion pumps). IHE PCD has identified use cases within the recent Service-oriented Device Point-of-care Interoperability (SDPi) White Paper[14], in which devices exchange software and hardware configuration details (UC.33, UC.194 and UC.199) to facilitate biomedical equipment management.

2.2.1.3 IHE ITI Configuration Management White Paper

In 2007, IHE ITI began to draft a Configuration Management White Paper[15] that proposed extending the DICOM LDAP model to HL7 v2 and XD* web services. Although this was not published as an IHE White Paper, its development fed into other work products, and was considered in the development of this white paper.

2.2.2 DICOM

One of the earliest attempts to standardize system configuration was within the Digital Imaging and Communications in Medicine (DICOM) Standard.

2.2.2.1 Configuration Management Profiles

In 2001, DICOM convened an ad hoc group on configuration management that developed use cases and a data model that led to the development of Supplement 67, Configuration Management, which was introduced into the DICOM standard in 2004[16].

Despite leveraging an existing LDAP infrastructure for campus configuration management support, a review of DICOM conformance statements reveals that most products do not support DICOM Application Configuration Management Profiles.

Poor adoption of LDAP for configuration and their engineering-centric nature are among the factors that have inhibited the acceptance of the DICOM Configuration Management Profiles in the marketplace.

2.2.3 Other

Other Configuration Management worth noting include:

- Interface definition language (IDL)[17], such as Web Services Description Language (WSDL) or Object Management group (OMG)

[14] https://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_SDPi_UseCases_Rev1-1_Pub_2019-11-01.pdf
[15] ftp://ftp.ihe.net/IT_Infrastructure/iheitiyr5-2007-2008/Technical_Cmte/Whitepaper_Work/Configuration/Config-Whitepaper-Outline04.doc
[16] http://dicom.nema.org/medical/dicom/current/output/html/part15.html#chapter_7
[17] https://en.wikipedia.org/wiki/Interface_description_language

- Universal Description, Discovery and Integration (UDDI) OASIS[18] standard that is no longer maintained
- WoT (Web of Things) Thing Description[19], a work item from the W3C Working Group, recently open for public comment
- FHIR CapabilityStatement resource and its expected publication on the metadata endpoint of a server[20]
- FHIR Endpoint resource[21] describes the technical details for how to connect to a FHIR server, and for what purposes
- mCSD, Mobile Care Services Discovery, provides a provides a RESTful interface to discover Care Services[22]; endpoint services could be managed in a similar manner
- DICOMweb includes a WADL Retrieve Capabilities Transaction, a machine-readable description of the service(s) implemented by an origin server[23]
- IEEE 11073[24] contains configuration specifications for point of care / personal health devices
- Configuration Management with SNMP (Simple Network Management Protocol, snmpconf)[25]
- Key Management Interoperability Protocol (KMIP)[26]
- Universal Plug and Play (UPnP)[27], a set of networking protocols supporting zero-configuration and automatic discovery in local area networks
- Web Services for Management (WS-Management) Specification, a SOAP-based protocol for the management of servers, devices, applications and various Web services[28]
- DNS Service Discovery (DNS-SD) standardizes DNS programming interfaces, servers, and packet formats to browse the network for services[29]
- Commercially available or open-source products that provide similar services

[18] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec
[19] https://www.w3.org/TR/2020/PR-wot-thing-description-20200130/
[20] http://hl7.org/fhir/http.html#capabilities
[21] https://www.hl7.org/fhir/endpoint.html
[22] https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_mCSD.pdf
[23] http://dicom.nema.org/medical/dicom/current/output/chtml/part18/sect_8.9.html
[24] https://en.wikipedia.org/wiki/ISO/IEEE_11073
[25] https://datatracker.ietf.org/wg/snmpconf/about/
[26] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
[27] https://openconnectivity.org/developer/specifications/upnp-resources/upnp/
[28] https://www.dmtf.org/sites/default/files/standards/documents/DSP0226_1.2.0.pdf
[29] http://www.dns-sd.org/

3 Use Cases

The current state use cases below touch upon the impact of unaccounted endpoint connectivity details, in which information must be collected and reconstructed.

The desired state introduces a standard data format and interface as a basic service to catalogue and search for connectivity details. This offers the potential to reduce the time and effort spent in the discovery of HL7 v2, XD*, DICOM and FHIR endpoint details.

3.1 Use Case #1 - New Single System Implementation

A new system is introduced into an existing enterprise that requires configuration to interface with other systems and vice-versa.

Implementation of a new system, whether a modality, such as an Ultrasound system, or an Information Management system, such as a Cardiovascular IT system requires exchanging technical details of connectivity to integrate within the existing enterprise.

3.1.1 Current State: New Single System Install

An institution interface analyst or system administrator is assigned to the project (departmental integrator). This may be formal or informal. Larger projects may also involve a project management resource.

Interface connectivity to existing systems is determined by the departmental integrator and vendors based on institution policy, use cases, departmental workflow and feature availability within the new and peer systems.

Endpoint configuration details are collected from the existing systems by the departmental integrator, potentially with the assistance of vendors.

The vendor configures the new system and the institution integrator coordinates the configuration of existing systems with vendors.

The configured interfaces are tested by the vendor and departmental integrator.

Any errors identified through testing are corrected by the departmental integrator and vendors. Errors may be due to incompatibilities, errors or missing features (i.e., an existing EKG cart is missing a DICOM license option).

The new system is cut into production and institutional and vendor team members are re-deployed to other projects. New teams take over responsibility for service and maintenance.

3.1.2 Desired State: New Single System Install

During the planning phase, the institution interface analyst reviews the new system specifications and compares them to information within a human readable SNIF retrieved from the repository, discovering that the new system may be undersized based on the number of existing endpoints and that some of the existing systems have incompatible interface versions.

The vendor is provided relevant entries from the institution's SNIF. Mismatches are reviewed with the vendor integrator and the implementation plan is modified to ensure desired connectivity between the new and existing systems is achieved.

During implementation, relevant SNIF entries are imported into the new system, avoiding manual entry and typographical errors. The new system is created in the institution's SNIF data source and its SNIF parameters are retrieved by the owners of the existing systems, identified in SNIF, to assist in TLS certificate exchange and connectivity testing.

3.2 Use Case #2 - Service

A service disruption between two or more endpoints may be caused by a network change or disruption, device repair swap-out, proactive service, software update, software anomaly, or system hang. Troubleshooting and repair frequently requires knowledge of the technical details associated with each endpoint interface.

3.2.1 Current State: Service

An institution interface analyst or system administrator responds to the service disruption. In evaluating the disruption, the interface analysist requires endpoint interface details to perform triage. The interface analyst spends time researching technical details of each interface in order to assess availability and identify vendors to engage in addressing the problem. Once engaged, vendor(s) may require additional interface details, depending on the completeness of the initial discovery performed by the institution.

Through iterative testing and gathering of information by those involved, the root cause of the disruption can be determined and addressed.

In cases where the solution requires an interface change, interface technical details are often modified, and the new system endpoint configurations are not catalogued.

3.2.2 Desired State: Service

In the initial triage of a service disruption, or in planning proactive service, the institution system administrator searches and retrieves interface connectivity details for the effected systems registered in the SNIF repository and immediately focuses activities based on known security profiles, network addresses, ports and departmental contacts documented within the SNIF.

In the case of a device repair swap-out, the spare is pre-configured in the biomed department before the physical swap-out, based on the SNIF, reducing re-configuration time.

4 Profile Proposal

4.1 Description

The objective of a SNIF Profile is to define a standard resource for institutions to catalog, search and access endpoint configuration details. SNIF is initially intended as a content profile with a basic coordinated infrastructure that serves information sharing needs.

In one deployment alternative, the SNIF data source would exist as a centralized service, such as an opensource, lightweight application. A second deployment alternative could be to pair the SNIF data source with a network management system. Each of these deployments establish an authoritative source of technical connectivity details; each also implies a dedication of healthcare institutional resources to maintain the catalogue.

A third deployment alternative could be a vendor assisted resource, in which products catalog and expose connectivity details in a standardized manner. In this alternative, products expose their connectivity details, as well as the connectivity details of registered peers within that product. This alternative potentially reduces healthcare institutional resource overhead, eliminates manual entry, and offers a method to automatically catalogue connectivity details of legacy products. This alternative; however, potentially introduces multiple SNIF data sources throughout the ecosystem. Without an authoritative source, healthcare institutions would be forced to manage duplicate and conflicting information (e.g., two Creators attempt to create or update information for the same endpoint entry).

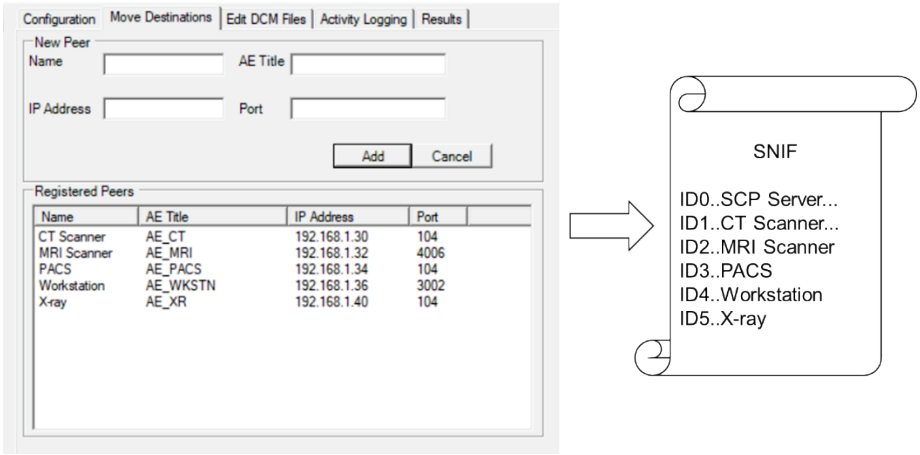


Figure 4.1-1: Vendor Assisted Model

Figure 4.1-1 depicts a fictional “DICOM SCP Server” that translates and exposes the connectivity details of itself and its registered peers into a standardized SNIF format (screen capture courtesy of DVTk QR SCP Emulator 5.0.1).

4.2 Process Flow

In this scenario an application exposes existing, endpoint configuration details in a SNIF that is accessible to the institution in a standardized manner.

At installation, the vendor enters endpoint configuration details in the application’s user interface. Configuration details are translated into a common SNIF format. From there, they could be made available for search and retrieval in an onboard SNIF repository and/or transmitted to centralized SNIF repository.

Actors retrieve SNIF connectivity details.

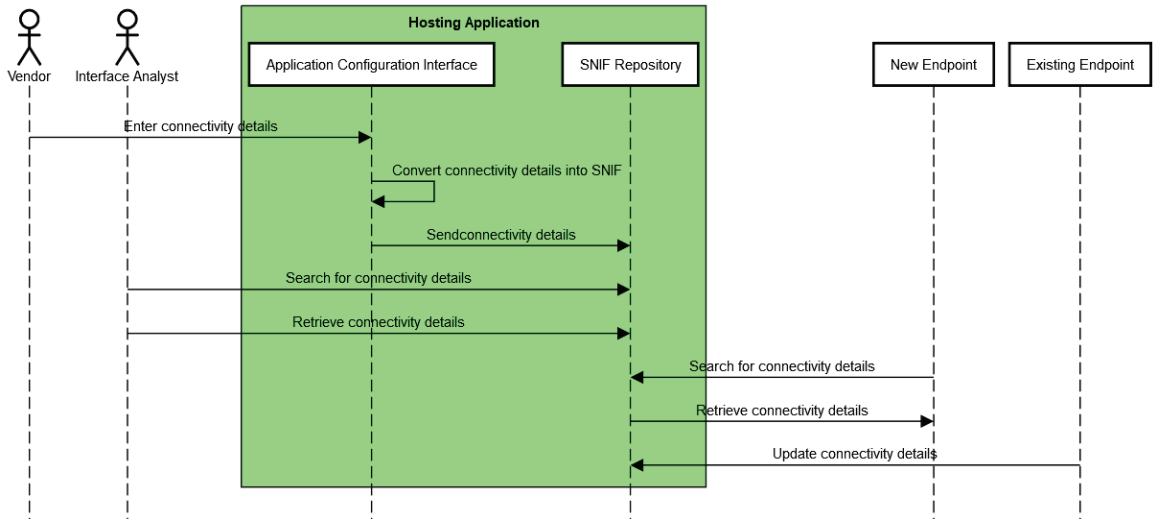


Figure 4.2-1: SNIF Process Flow, Vendor-Assisted

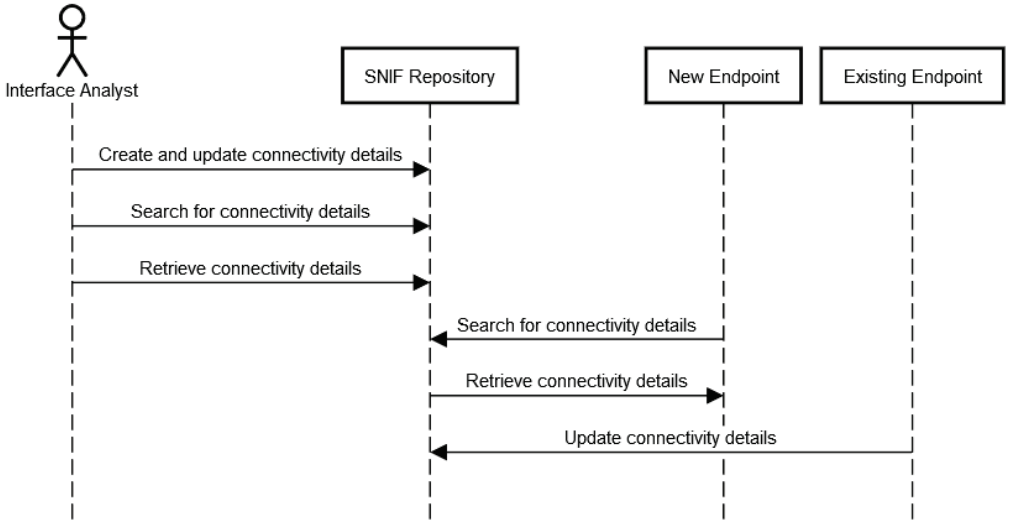


Figure 4.2-2: SNIF Process Flow, Centralized Repository

4.3 Security Controls

The SNIF will require a proper security model based on local security policy, considerations and threat model. It is expected that a range of security models are possible. Although the SNIF is not intended to include a specific security model, it is expected that SNIF will group actors with actors from the IHE Audit Trail and Node Authentication and will need a capability of access control and secure communications.

Other IHE Integration Profiles complementary to SNIF are available (e.g., Enterprise User Authentication, Document Digital Signature, etc.).

ATNA expects that local governance determines which methods of user authentication will be used, however token, federated or Kerberos-based authentication methods, as in IUA, XUA or EUA could be also employed.

A SNIF creator may digitally sign a SNIF, supporting the Digital Signature (DSG) Content Profile as a Document Source. When a SNIF consumer needs to verify a Digital Signature, it may retrieve the digital signature document and may perform the verification against the signed document content.

4.4 Actors

4.4.1 SNIF Content Creator

The Content Creator is responsible for populating, deleting and updating endpoint configuration details within the SNIF that will be shared or exchanged between other IHE actors.

A stand-alone SNIF Content Creator could be network planning software, utilized in the planning of an implementation (as in 3.1 above) that creates planned SNIF content within the SNIF Repository. In a more likely scenario, the SNIF Content Creator would be grouped with other actors, such as a Modality, Audit Consumer, or Document Repository, in which the actor creates or updates its own configuration details within the SNIF Repository.

4.4.2 SNIF Repository

The Repository is responsible for the persistent storage of the SNIF. In addition, the Repository could query existing SNIF Content Creators for updates based on a polling interval defined by local policy.

As with the SNIF Content Creator, an opensource or network management system could act as a stand-alone SNIF Repository. Other scenarios could imagine the SNIF Repository grouped with an Image Manager/Archive or an Initiating/Responding Gateway.

4.4.3 Integrated SNIF Content Creator/Repository

The Integrated SNIF Content Creator/Repository combines the functionality of the Content Creator and Repository Actors into a single actor that exposes peer endpoint configuration details configured on that server.

For example, an ECG Manager could act as a SNIF Content Creator by translating ECG cart endpoint connectivity details into SNIF and exposing these to Content Consumers as a Repository.

For viability, data management policies are required to deal with duplicate or conflicting SNIF content from external Content Creators. For example, a repository could choose to refuse Create/Update transactions, merge Create/Update transactions with existing SNIF entries, present duplicate SNIF entries in query responses, or flag conflicts for user resolution.

In addition to security (see Section 4.3), Digital Signatures provide a clear source and timestamp that aids in establishing an authoritative SNIF source.

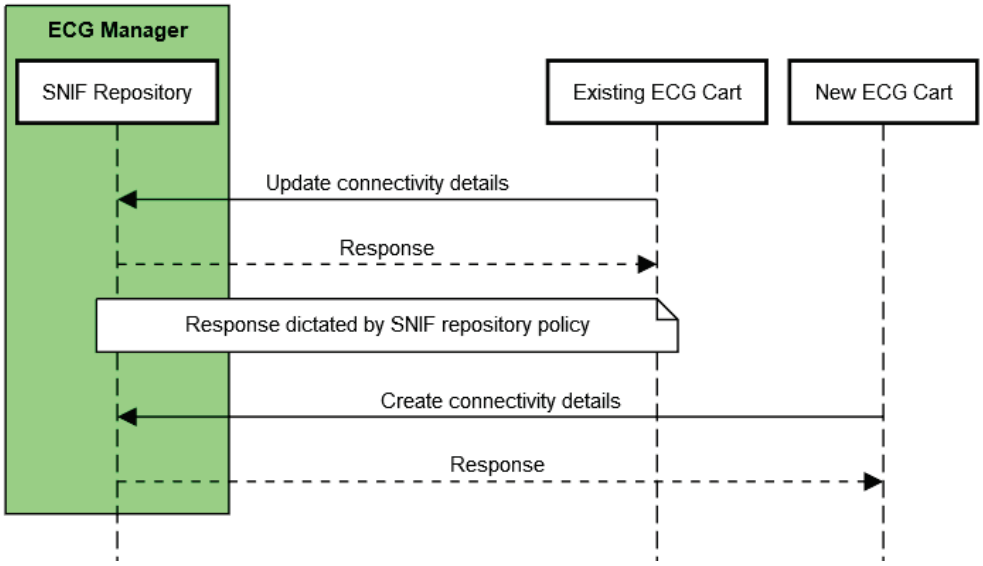


Figure 4.4.3-1: Application of a Data Management Policy

4.4.4 SNIF Content Consumer

The Consumer is responsible for queries based on connectivity details, and retrieval of SNIF meeting query criteria. Queries would be based on data elements described in the data model in Section 4.6.2.

For example, a Protocol Manager could be grouped with SNIF Content Consumer in order to retrieve connectivity details for Modality actors supporting DICOM protocol object transfer.

4.4.5 Grouping

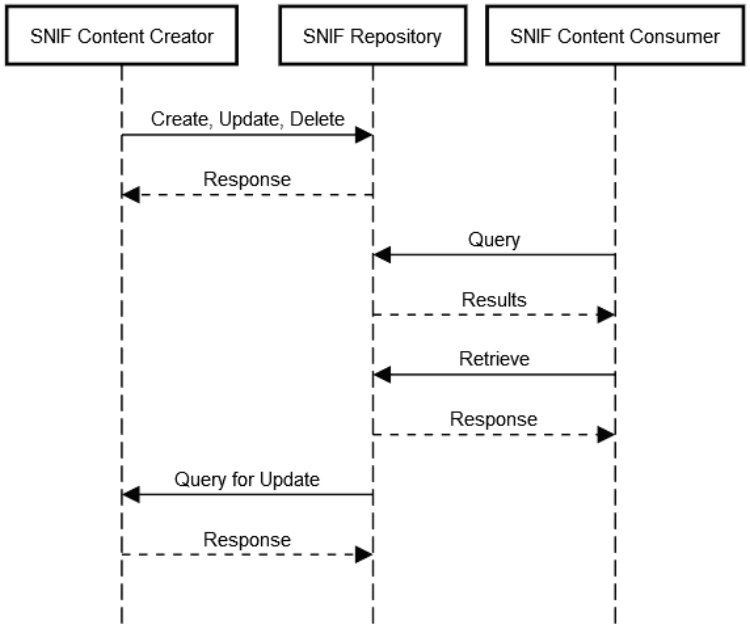
It is envisioned that Security Controls (Section 4.2) warrants grouping as below. An actor from this profile (Column 1) shall implement all the required transactions and/or content modules in this profile in addition to all transactions required for the grouped actor (Column 2).

Table 4.4.5-1: SNIF Required Actor Groupings

SNIF Actor	Profile/Actor to be grouped with
Content Creator	ATNA / Secure Node or Secure Application
	CT / Time Client
Repository	ATNA / Secure Node or Secure Application
	CT / Time Client
Content Consumer	ATNA / Secure Node or Secure Application
	CT / Time Client

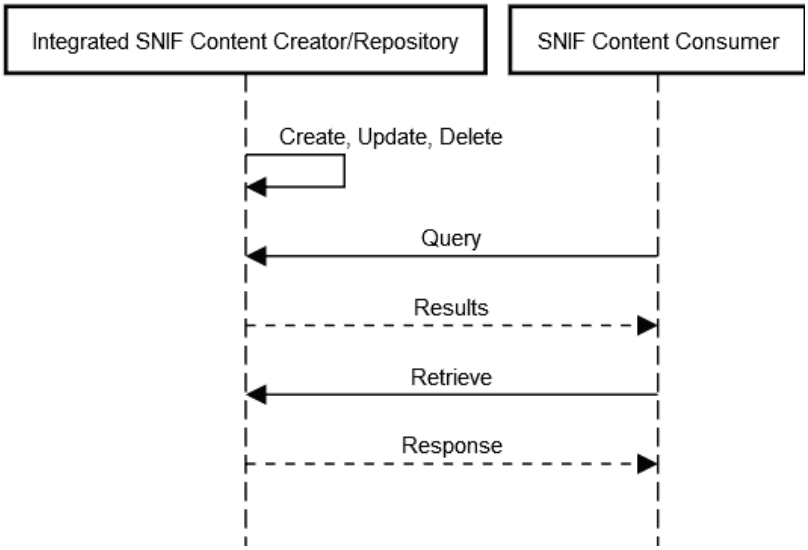
4.5 Transactions

Transactions support the basic population of the creation and management of the SNIF.



480

Figure 4.5-1: SNIF Transactions for Individual Content Creator, Repository and Consumer Actors



485

Figure 4.5-2: SNIF Transactions for Integrated Content Creator/Repository and Consumer Actors

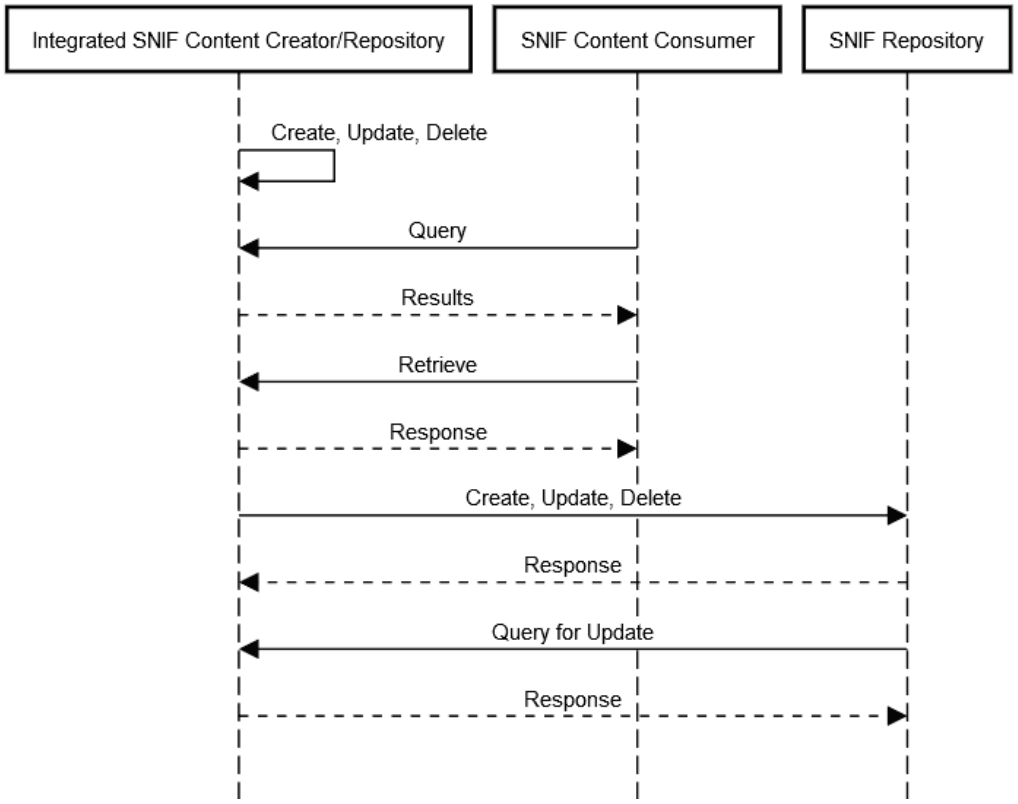


Figure 4.5-3: SNIF Transactions for Integrated Content Creator/Repository and Consumer Actors with a Central Repository

4.6 Data Model

4.6.1 SNIF Repository Data Model

A SNIF Repository requires a data model in order to be distinguished from and registered within other SNIF Repositories.

Table 4.6.1-1: Elements in the SNIF Data Model

Element	Description
Identifier	Unique identifier of the SNIF Repository used across systems
Name	Identifiable name of the SNIF Repository
Managing Organization	Organization that manages this SNIF Repository
Contact	Contact (owner) details for this SNIF Repository
Period	Interval this SNIF Repository is expected to be operational
Last Update	Last update of this SNIF Repository
Status	Planned, Test, Production

4.6.2 SNIF Contents Data Model

Each standard utilized in IHE profiles offer unique levels of complexity. For a profile to be simple, yet robust, a common data model should be established.

The table below is non-comprehensive and intended as a starting point for the SNIF Profile. The four columns to the right (FHIR, HL7 v2, DICOM, XD*) contain the relationship of each element to that standard, each described as required ("*"), strongly recommended ("x"), recommended ("o") or not applicable (empty). Data elements within the model are grouped by Administrative, Operational and Technical, posing an opportunity to profile existing standards as appropriate by group.

This initial data model does not address cardinality, although it is recognized that one address may offer multiple services (e.g., DICOM Modality Worklist, Performed Procedure Step, Storage and Storage Commit).

Finally, it is also recognized that some of elements below are better represented through encoding for machine readability.

Table 4.6.2-1: SNIF Data Model Elements - categorized

Element	Description	FHIR	HL7 v2	DICOM	XD*
Administrative					
Identifier	Unique identifier, used across systems	*	*	*	*
Name	Identifiable name of the endpoint	*	*	*	*
Managing organization	Organization that manages this endpoint	*	o		*
Contact	Contact (owner) details	*	*	*	*
Operational					
Period	A time period (defined by a start and end date/time) that the endpoint is expected to be operational	o	o	o	o
Time zone	Time zone of the endpoint	o	o	o	o
IHE Profiles & Actors	Profile/actor pair(s)	*	*	*	*
IHE Transaction & Roles	Supported transactions and roles	o	o	o	o
Status	planned, test, production	o	o	o	o
Receiving/Sending Facility	HL7		x		
Receiving/Sending Application	HL7		x		
Integration Guide	Site/product specific documentation, such as Implementation Guide, HL7 or DICOM conformance statement, IHE integration statement	o	o	o	o
Technical					
Connection type	Endpoint protocol or standard	*	*	*	*
Connection type version	Endpoint protocol or standard version	x	x		
Transport	TCP/IP, HTTP, MLLP		*	*	

Element	Description	FHIR	HL7 v2	DICOM	XD*
Service details	DICOM PS3.15 Annex H[30], DICOMweb Capabilities[31], FHIR Capability Statement[32], HL7 messages supported, DIMSE services	o	*	*	o
Address	Address for connecting to this endpoint (e.g., URL, IP/hostname, port)	*	*	*	*
Connection type security description	IHE ATNA Options[33] (CP-ITI-1151)	*	*	*	*
Connection security certificate management	Signed Direct Comparison, Certificate Authority	*	*	*	*
Transmission	Synchronous or asynchronous communication	o	o	o	o
Application Entity	DICOM AE title			*	

4.7 Future Profile Extensions

This white paper scopes the minimum viable profile for cataloguing, search and retrieval of endpoint connectivity details for standards commonly profiled within IHE.

Once adopted, it is envisioned that future revisions to the SNIF Profile would include transactions to establish a plug-and-play environment in which discovery and registration establish systems' configuration without human intervention.

For example, a system newly introduced to a network performs an auto-discovery to identify the SNIF repository, self-registers and automatically retrieves and configures appropriate connections based on purpose and capabilities.

[30] http://dicom.nema.org/medical/dicom/current/output/html/part15.html#chapter_H
[31] http://dicom.nema.org/medical/dicom/current/output/html/part18.html#sect_8.9
[32] https://www.hl7.org/fhir/capabilitystatement.html
[33] https://gazelle.ihe.net/files/CP-ITI-1151-04-ballot54.pdf