DAF SMTP for IHE: Issue of Scope

By Stephen Beller, PhD on January 6, 2015

As requested during the Jan 5, 2015 DAF IHE meeting, this paper discusses five key points about the scope of SMTP as a transport model for DAF IHE: (1) Widespread acceptance of the SMTP transport model standard; (2) Existence of a DAF SMTP query model; (3) Transparency SMTP provides; (4) Security and reliability of SMTP; and (5) Benefits of a balanced approach to transport. Issues about complex relationships and funding are also raised.

1) SMTP: A Viable, Widely Recognized, Transport Model Standard

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission. It was defined by RFC 821 in 1982 and was last updated in 2008 with the Extended SMTP additions by RFC 5321 - which is the protocol in widespread use today. IHE and DAF USA recognize SMTP as a viable transport model standard. SMTP is recognized by HIMSS, ONC's DIRECT Project, MU2 and the 360X closed loop referral initiative.

1.1) IHE

Here's a quote from the [IHE IT Infrastructure White Paper - Health Information Exchange: Enabling Document Sharing Using IHE Profiles](), published January 24, 2012:

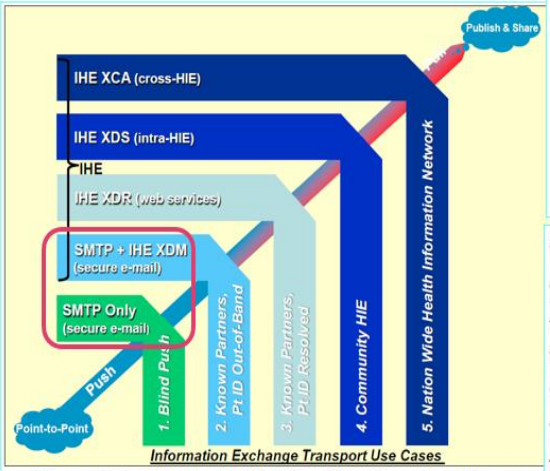

Figure 3-2: Document Sharing Use Case Continuum

2.8 Document Sharing Models

IHE has enabled three distinct Document Sharing Models that share the principles in this section. Because the principles are the same it is relatively simple to implement more than one model to accomplish multiple objectives. The three models are:

- Direct Push – in this model, clinical content in the form of documents and metadata is sent directly to a known recipient, or published on media for delivery

3.1.2 Cross-Enterprise Document Media Interchange (XDM)

The Cross-Enterprise Document Media Interchange (XDM) profile addresses situations where the electronic exchange of clinical information does not rely on networked connections between the parties exchanging the information. In these cases, electronic media (such as CDs and USB drives) or email may be employed to transport the data from one system to another.

The XDM e-Mail option is a logical advance for directed e-mail exchange that provides content packaging and metadata to enable accurate processing. The XDM profile has been adopted in national exchange specifications such as the USA defined "Direct Project".

1.2) DAF USA White Paper

Here's a quote from the white paper—IHE Patient Care Coordination (PCC) White Paper - A Data Access Framework using IHE Profiles Revision 1.0 (authored by Nagesh Bashyam and Keith Boone)—that was DAF submitted to IHE on March 28, 2014:

Queries using SMTP and S/MIME (SMTP)

Currently there is limited use of SMTP (IHE XDM profile has an SMTP option) stack for data access; however the SMTP stack may play a role in asynchronous query implementation. A derivative of the SMTP stack (i.e., Direct) is required for Meaningful Use stage 2 in the US due to which many EMR systems are supporting the STMP stack as one of the protocols to enable push based messaging. The S/MIME standard is used to structure the package in the SMTP stack. The package itself leverages other standards and formats to further define the data structures.

1.3) HIMSS

Here are quotes from the Practical Guidance to Implement Meaningful Use Stage 2 Secure Health Transport for Certification and Meaningful Use by the EHR Association Standards and Interoperability Workgroup indicated that SMTP is the only transport model required for meaningful use EHR certification:

Required Certification: (a) Direct SMTP Only
EHR vendors have a variety of implementation strategies, as long as an S-MIME encrypted E-mail is received by the test tool.

Optional Certification: (a+b) Direct with XDM
This certification is optional in addition to (a), **not** instead of (a), as (a) is minimally required.

Optional Certification: (b+c) XDR (with SOAP)
This certification is optional in addition to (a), **not** instead of (a), as (a) is minimally required.

1.4) DIRECT Project

Here's a quote from the DIRECT Applicability Statement for Secure Health Transport - Version 1.1 (July 2012):

Abstract

This document describes how to use SMTP, S/MIME, and X.509 certificates to securely transport health information over the Internet. Participants in exchange are identified using standard e-mail addresses associated with X.509 certificates. The data is packaged using standard MIME content types. Authentication and privacy are obtained by using Cryptographic Message Syntax (S/MIME), and confirmation delivery is accomplished using encrypted and signed Message Disposition Notification. Certificate discovery of endpoints is accomplished through the use of the DNS and LDAP. Advice is given for specific processing for ensuring security and trust validation on behalf of the ultimate message originator or receiver.

Having shown that SMTP is viabile, and even required transport model, I will now discuss other reasons to classify SMTP as in-scope for DAF IHE.

2) SMTP's Query Model

One of the reasons stated for making SMTP out of scope for DAF IHE is that there is no query profile for SMTP. Certain individuals in workgroup meetings claimed that this assumed functionality gap is reason enough to classify SMTP as out of scope.

The DAF White Paper's gap analysis, shown in the grid on the next page, indentifies SMTP as having gaps across the board. The problem is, however, this assertion is incorrect because it fails to indicate the DAF over Direct sub-workgroup (the "SWG") determined a query profile months ago.

The DAF SMTP profile is one in which query parameters are stored in a file w/in an XDM package and transported via e-mail. A black box application retrieves the file, executes the query, and returns the results in standardized format in another XDM package. The query parameters will be based on any standardized vocabulary and syntax that the main DAF WG selects, including FHIR, CDA and other standards that can be

implemented asynchronously. SOAP and REST also have gaps. It therefore stands to reason that such gaps, per se, are not adequate reasons for calling a transport model out-of-scope; the White Paper should be modified accordingly.

815 These models are used regardless of the kind of governance applied to the systems exchanging information.

Table 5-1: Implementable Specifications

Data Access	Behavior Model	Network Transport	Implementable Information Model	IHE Profile	
				Patient	Population
Patient Demographics	Request/Response	MLLP	HL7 V2 ADT	PIX/PDQ	Gap[1]
		SOAP	HL7 V3 Patient Administration	PIX/PDQ V3 XCPD (Federated)	
		REST	FHIR Patient	PDQM	
	Publish/Subscribe	SOAP	HL7 V3 Patient Administration	Gap[2]	
		REST	FHIR Patient		
Encounter Documents and Metadata	Request/Response	SOAP	ebXML RIM+CDA	XDS/XCA	MPQ
		REST	FHIR+CDA	MHD	Gap[3]
		SMTP	Gap[10]		
	Publish/Subscribe	SOAP	ebXML RIM+CDA	DSUB	Gap[4]
		REST	FHIR+CDA	Gap[5]	
		SMTP	Gap[10]		
Detailed Clinical Data	Request/Response	SOAP	HL7 V3 Care Record	QED[8]	Gap[6]
		REST	FHIR	Gap[7]	
	Publish/Subscribe	SOAP	HL7 V3 Care Record	CM[9]	
		REST	FHIR	Gap[7]	

Implementable information models are represented in the Message Semantics section describing transactions in Volume 2 or in Content Modules found in Volume 3.

3) SMTP's Query Transparency

Another issue relates a problem the SWG co-lead, Joel Ryba, had with the direction of DAF. This relates to the issue of trust discussed during the last DAF IHE meeting.

I first want to make the point that this issue was ignored in the DAF IG_Project Team_2014 12 29 Notes for Review.docx document, which states: "The DAF DIRECT community subgroup lead for document based query, Joel Ryba, reported that there did not appear to be a case for creating a DIRECT transport option as another IHE document metadata based query profile."

Instead, Mr. Ryba wants DAF over Direct for document queries to promote greater transparency. He told me he was displeased that IHE XDS and the future FHIR implementations will be governed by policy and implemented by EHR and HIE vendors in a way that makes it a "taking of the data" via a PULL/QUERY rather than "peer to peer questions," rather than seeing it as a "take of the data".

He sees this issue as being about enabling exchange in ways not subject to policy with greater restrictions than required by law. The current IHE XDS and the future FHIR implementations will be governed by policy and implemented by EHR and HIE vendors in a way that makes it a "taking of the data". The policy will be some "consent to access", opt-in, or opt-out policy that is incompatible with other policies in other jurisdictions. The query/pull policy will not enable normal transactions that are done via phone and fax, or even now by manual Direct, every single day. The system implementations of these protocols will reinforce this with how it records the query in the audit log and how it configures the RBAC (e.g. consent) policy in the system.

He perceives DAF over Direct as different because DAF describes a query accurately as a request and response. The business rule evaluation for sharing was on the entity responding. By using Direct, the request was made peer to peer, the evaluation was done independently, and the response was made peer to peer. In the end of the day, query is synonymous with question. This enables organizations to do business of PULL/QUERY based on their own rules, the way they do today. Legally, but without the restrictions of a statewide policy that is designed around organizations not having other relationships and business rules that allow the data to flow legally.

He believes that you will never get either technologist or policymakers to see XDS or FHIR as a "peer to peer questions" rather than seeing them as a "take of the data". That, combined with the pervasiveness of Direct, was the reason Direct seemed best to solve for the problem of lack of knowledge of the policymakers.

DAF SMTP is a way to promote this kind of transparency and this is another reason for it being in-scope.

4) SMTP's Security and Reliability

Protection of sensitive health information is crucial, as is the reliable delivery of that information. SMTP with S/MIME, along with Message Delivery Notification (MDN), provides the high level of security reliability.

4.1) SMTP + S/MIME Security

- S/MIME encrypts message body and attachments, but not message headers
- Transport layer encryption is an additional layer done to a server MTA using TLS or using an edge protocol such as POP3S or encrypted IMAP
- Encryption between SMTP servers (MTA or message transfer agents) is also applied using STARTTLS
- Messages can be encrypted to people, as defined in the IHE HPD directories, or to servers (endpoints)
- The highest level of security has no middle layer in which to expose the message; it can only be decrypted by the authorized recipients, this is end-to-end encryption using the Simple SMTP model described by DIRECT
- Only the possessor of the private key (owner) can decrypt the message, any other method exposes the message to a cryptographic Man in the Middle Attack (MITM), a well-known threat.

4.2) Reliable Delivery

One model for enabling reliable delivery of SMTP messages is described in the Implementation Guide for Delivery Notification in Direct - Version 1.0, 29 June 2012 publication. Its guidance "…provides a high level of assurance that a message has arrived at its destination and outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken…to provide success and failure notifications to the sending system."

5) Case for a Balanced Approach to DAF Transport

There is also good reason to have a balanced transport approach that includes both the web and Internet transport models:

- The web provides the benefits and advantages of relatively complex use of SOAP and RESTful services in the cloud. This is important for use cases that focus on enabling tightly-coupled integration networks to:
    - Maintain central control of data storage, processing and transport
    - Utilize centralized resources
    - Pull data via dumb endpoints with a smart middle
    - Communicate in stable, high bandwidth environments
    - Constrain query transparency.
- The Internet, on the other hand, provides the benefits and advantages of a relatively simple use of reliable and efficient SMTP plus S/MIME. This is important for use cases that focus on enabling loosely-coupled integration networks to:
    - Maintain local control of data storage, processing and transport
    - Reduce architectural complexity and demands central servers through utilization of local resources
    - Push data via smart endpoints with a dumb middle
    - Communicate in all situations, including unstable, intermittent or low bandwidth environments
    - Foster query transparency
    - Execute queries offline, send the payload via e-mail required by MU2, and not rely on a browser and web services (due to security or other concerns).

Implementations that enable both web services and SMTP would cover both use cases:

- Increase the likelihood of responder compliance by fostering trust/transparency
- Broaden communication options
- Open up business opportunities for, and stimulate innovation among, developers/vendors and consultants
- Provide choice and a hedge against transport failure and/or security breach
- Eliminate any possible appearance of unethical or illegal market influence (e.g., restraint of trade by standards manipulation).

6) Dealing with Complex Relationships and Funding Issues

There was a general consensus at the last Main DAF work group meeting that the group is unopposed to DAF over Direct and the SWG's efforts. However, several group members stated that IHE lacks the money and resources to develop the SMTP query profile, and that there is only enough funding for web services profiles. In addition, since the main work group demanded that the SWG use FHIR vocabulary, it means that HL7 is now involved along with S&I and IHE. I find this all rather confusing in terms of the distribution of requirements, responsibilities and resources.

So, my question is this: How can work on a DAF IHE SMTP profile obtain funding and technical support? Our organization is prepared and competent to take a lead role.

Conclusion

I assert that there is every reason to include *both* SMTP and web services as DAF IHE transport standards. My assertion is justified by SMTP's widespread acceptance, viable query model, and important use case benefits. I contend that there should be funding and technical support for both transport standards.