Direct, DirectTrust, and FHIR: A Value Proposition

August 10, 2017

Authors: Grahame Grieve, HL7 Product Director for FHIR; David Kibbe, Luis Maas, Greg Meyer, and Bruce Schreiber, members of the DirectTrust Policy Committee

Introduction

FHIR is a new standard that defines a web API and related specifications for health data exchange. Direct is an existing federal standard that is widely used in the USA for the exchange of healthcare data. There are differing views across the healthcare system as to the correct relationship between the two standards and communities. This white paper proposes a way to understand how the FHIR and Direct communities and technical specifications for each standard should relate to each other. The authors describe two main ways to use the existing Direct and DirectTrust assets with FHIR: pushing FHIR resources in Direct Messages, and; using DirectTrust certificates with the RESTful API.

Note: this document is published by DirectTrust, and was prepared with the assistance of Grahame Grieve, the product director for the FHIR standard, as a position paper for consideration by the Direct and FHIR communities. It is not yet formally endorsed by HL7, or by the FHIR community.

Background

Direct is a protocol stewarded by the Office of the National Coordinator for Health IT (ONC) and the Direct Project community that describes a secure way to send content from one healthcare participant to another, using a secure protocol with verified identities. Direct specifies a trusted, secure network that leverages the sMIME/SMTP protocol to create an independent system. The Direct Protocol is payload agnostic connecting endpoints with non-persistent connections.

DirectTrust is a collaborative non-profit association that supports secure, interoperable health information exchange via the Direct message protocols. DirectTrust has created a "trust framework" and a service delivery network that extends use of Direct exchange to over 100,000 health care organizations and 1.5 million end points (see map: https://www.directtrust.org/directory-coverage-map/). The DirectTrust trust framework supports both provider-to-provider Direct exchange and bi-directional exchange between consumers/patients and their providers, and includes a Public Key Infrastructure, PKI, for strong identity assurance.

DirectTrust has established and operates a voluntary Accreditation and Audit program serving Direct implementers/service providers, available for: 1) Health Information Service Providers (HISPs), 2) Certificate Authorities (CAs) and, 3) Registration Authorities (RAs). There are currently 45 such DirectTrust accredited service providers in 2017, each of whom must pursue re-accreditation every two years.

FHIR is a community that is developing a standard for health data exchange through exchanging 'resources' which are well described modular packets of healthcare data. It describes a web API and related standard that allows for healthcare applications to exchange data in a consistent interoperable fashion. As a new standard, FHIR offers a basis for exchanging data in the future, and many implementers have indicated a desire to use it.

C-CDA (Consolidated CDA Implementation Guide) is a mature specification from HL7 that describes a document with embedded data that has been widely implemented due to Meaningful Use rules. FHIR differs from C-CDA in several key respects: as well as defining a document format, FHIR describes other usages, principally the Web API, which means that information represented using FHIR can be used in many more ways than C-CDA.
Health Level 7 (HL7) is the Standards Development Organization that hosts both the FHIR community and the C-CDA standard, and publishes the actual standard that the community agrees to.

HL7 is an ANSI accredited international standards organization based in the USA that focuses on data exchange standards for healthcare applications. FHIR is the latest in a line of standards that are widely deployed throughout the healthcare institutions around the world.

The Perception Challenge
The FHIR community's current focus is 'perimeter interoperability' – that is, exchange of data outside the institution, either with patients/consumer directly, or between institutions. In the USA, most of the focus around FHIR has been consumer to business (C2B) rather than business to business (B2B). This focus is because institutions have their internal integrations and some external exchanges already in place, whereas C2B is where immediate value can be extracted and may lead to a marketplace for apps.

The primary use of the Direct protocol is for exchanging data between clinicians and support staff in institutions. Today, as a result of the Meaningful Use Program, Direct is commonly used to carry C-CDA formatted data between many institutions using version R2.1 of the C-CDA. There were over 98 million such exchanges via Direct in the DirectTrust network during 2016, and approximately 150 million transactions are expected in 2017. However, there is a perceived conflict between the current use and growth of Direct and the future use of FHIR. This perception exists even though Direct is content agnostic, and FHIR as a resource is transport agnostic.

FHIR does define a transport protocol – that is, the RESTful HTTPS API which is the most well-known and understood part of the FHIR specification. However, from the beginning, the FHIR community and specification has understood that not all problems can or should be solved by using a RESTful API, and so it has always described how to use other means for exchanging resources.

What FHIR does not do is describe a *secure* RESTful API. Implementers need to take the generic RESTful API, and deploy it using the appropriate security and trust protocols. What the appropriate choices are varies widely depending on the context. For practical reasons, many FHIR implementers have chosen to use TLS + SMART-on-FHIR as the basis for their security.

In recognition of this, SMART-on-FHIR is currently going through the process of elevation into a full HL7 standard, though it will continue to be one way to use FHIR, not the only way. SMART-on-FHIR is a profile of OAuth and OpenID Connect that describes how to implement these to authenticate and authorize the use of the FHIR API. However, an underlying trust framework is still needed. In addition, there is ongoing confusion about what it would mean to 'use FHIR with Direct' (or vice versa), when implementers might use one or the other, and how to use them together.

Value Proposition for Direct / DirectTrust's Trust Framework

Although the multi-functional FHIR API offers considerable flexibility for programmers, a distribution/connection/trust framework is still required, and setting this up involves considerable cost. SMART-on-FHIR, while useful as a tool for delegating authorization and authentication, is not itself a distributed trust framework – it still relies on some other application or framework to provide authentication and authorization.

The Direct community faced and solved a similar challenge several years ago, when participants needed to exchange certificates with each other to enable exchange, and to determine the trustworthiness of relying parties. Exchanging healthcare information securely and reliably requires a concrete but scalable mechanism for assuring security and trust for the exchange of electronic healthcare information, as well as for governance of the trust network that engages in the exchange, so that point-to-point verification is not required. Building such a network requires considerable investment in management, administration and technical verification mechanisms. Such investments cost substantial amounts of money – millions of dollars, though little public information is available to quantify the real total expenditure of the different existing networks.

DirectTrust provides scalable security and trust through legal contracts, formal policies, accreditation, and a PKI-based trust authority. DirectTrust's primary work has been centered on building the security and trust-in-identity layer for the operation of Direct exchange between providers of healthcare as well as between providers and patients and in governing those operations.

The Direct PKI-based trust authority greatly simplifies the distribution of X.509 digital certificates used in the process of Direct messaging to establish trust and encryption/decryption between relying parties to Direct health information exchanges. The DirectTrust infrastructure employs trust anchor bundles that add efficiencies by making it possible for entities such as hospitals and medical practices to assert adherence to security and trust policies and practices, obviating individual one-off negotiations or contracts with respect to controls for privacy, security, and trust in identity. The trust anchors are used to ensure trust of X.509 certificates held by HISPs on behalf of their customers to encrypt and validate the senders and receivers in the exchange of Direct messages and attachments over the Internet.

Because there is such expenditure involved in planning, setting up and maintaining trusted distribution networks, there is strong incentive to leverage existing networks as much as possible. For this reason, existing FHIR Implementations across the world use a wide variety of established infrastructure, including methods such as embedding FHIR resources inside HL7 v2 messages, or using XDS as a wrapper around the RESTful API.

Using existing communication infrastructure like those just mentioned is sometimes not appropriate where the fine grained bi-directional interactive nature of the FHIR API is necessary, but in many cases, information flow is uni-directional, or the granularity of exchange is fairly coarse, and it's in these situations that making use of existing distribution networks is a compelling idea.

There are two main ways to use the existing Direct and DirectTrust assets with FHIR:

- Push FHIR resources in Direct Messages
- Using DirectTrust certificates with the FHIR RESTful API

Pushing FHIR resources in Direct Messages

In this scenario, the sender gathers up a set of resources that they wish to send to a recipient, packages them in a FHIR bundle, and sends it as a Direct message to the recipient, which unpacks the resources and processes them.

A separate specification "Sending FHIR resources in Direct Messages" (still under development) describes how resources can be sent in this fashion, and what obligations exist for the sender and receiver to ensure correct processing.

This approach is relevant where each exchange information flow is uni-directional, and a Direct-based trust network like that of DirectTrust exists between the source and destination (i.e. the source knows how to deliver to the destination). Where these conditions exist, using Direct to send messages saves implementers from recreating the same distribution management system, such as certificate and policy frameworks and trust agreements.

There are some additional technical advantages of Direct in the use cases where push makes sense over a typical request/reply, bi-directional exchange:

- The asynchronous nature of SMTP and built-in queueing in most SMTP implementations can lead to higher Quality of Service (QoS);
- The dynamic routing to end-points.

Using DirectTrust Certificates with the FHIR RESTful API

As discussed above, the FHIR API itself specifies no particular security arrangement. The focus of the existing implementation work on SMART-on-FHIR is around authorization mediated by a human as part of the interaction (C2B context). In this context, the authentication of the user is delegated to the authorizing server.

The existing work in the FHIR eco-system does not deal with establishing trust between systems. To authenticate system-to-system communication, some trust framework will be needed – either point to point agreement about certificates and other security tokens, or some mediated trust community will need to provide a framework in which these are managed.

The DirectTrust community could serve this role – this would enable the 100,000+ existing DirectTrust enabled institutions and 1.5 million identity proofed addressees at those institutions to allow connections between each other without the need for point-to-point agreements. Such an arrangement would also potentially save the FHIR community from the financial requirement to build a new trust framework by using one already proven to scale high identity assurance. Enabling this requires both technical and policy agreements.

A separate specification "Using certificates with the RESTful API" (still under development) describes how appropriate certificates can be acquired and used to secure RESTful APIs, and lays out a basic policy framework to allow any DirectTrust participant to automatically accept and process requests for data from any other participant.

Conclusion

The proliferation of FHIR implementations offers new opportunities to leverage existing investments in Direct and DirectTrust. We should play an active role in supporting the FHIR community so that their potential usefulness may be realised.

The leadership of both the DirectTrust community and the FHIR community should seek opportunities to build engagement between the respective communities to flesh out both the technical specifications detailed above, and their policy and adoption implications.