CXP – A Patient-Centric Document Transfer Protocol Supporting Federated Identity Management

MedCommons White Paper
March 2006

Abstract

CXP is a protocol for the structured and reliable exchange of standards compliant xml based Healthcare Records and Messages between Patients, Providers, Payors, and medical Devices. Based on SOAP and optionally, WS* standards, CXP achieves a high degree of security via support of both hardwired TLS connections and dynamic WS-*/SAML based operations over a federated identity network such as the Liberty Alliance or Microsoft InfoCard.

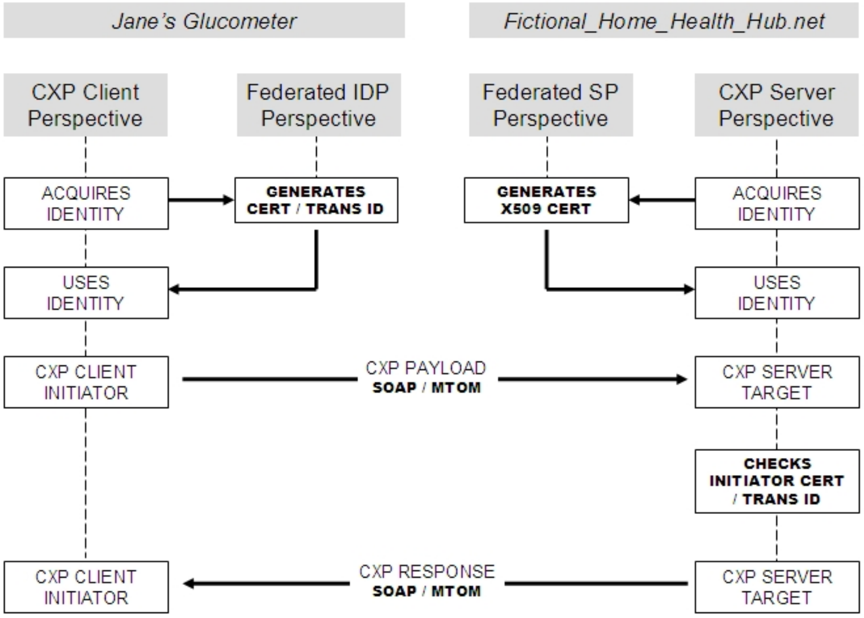
The payload in a typical CXP exchange is one or more structured XML documents, with additional unstructured document types (notably PDFs) included as attachments. The XML formats supported include CCR, and will cover CCD and CDA if applicable. The CXP Server often front-ends a document repository and may be configured to validate incoming payloads against specific XSD schemas, interact with one or more registries, or perform enterprise specific processing.

CXP Overview

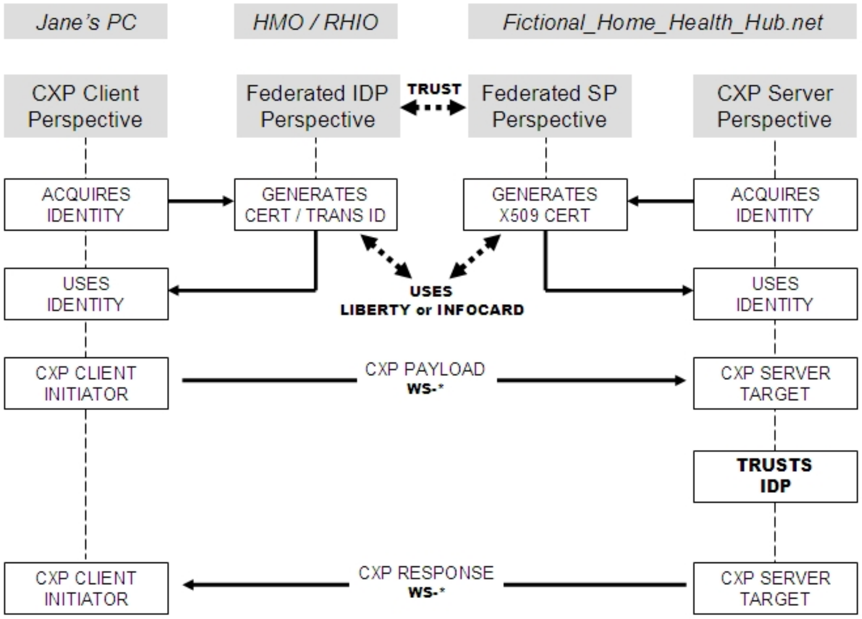
The Commons Exchange Protocol (CXP) is a TCP based end to end HealthCare Aware Protocol allowing two parties to structure a spontaneous and reliable constrained exchange of standards-based, patient-focused healthcare information. It can be utilized over plain http or SSL, over locked-down certificate based TLS connections, or preferably via a Federated Identity Management scheme such as the Liberty Alliance or Microsoft InfoCard, each with increasing levels of trust. CXP is defined on top of existing standards including SOAP with or without MTOM, and the WS-* family of web services protocols. CXP permits PHR and EHR vendors to utilize basic GET, PUT, and DELETE services to exchange and validate structured data and metadata in common formats including CCR, CCD, CDA, and any other XML based schema.

Use Cases

Importantly, the CXP interface afforded to PHR and EHR vendors is neutral with regard to the presence or absence of particular WS-* features including identity, security, and discovery services. This allows vendors to construct simple client implementations of their applications that assume only SOAP is present, yet lets larger enterprises, software vendors and service vendors to immediately gain benefits from additional complex services layered above CXP built around Liberty, InfoCard and WS-* supported protocols.

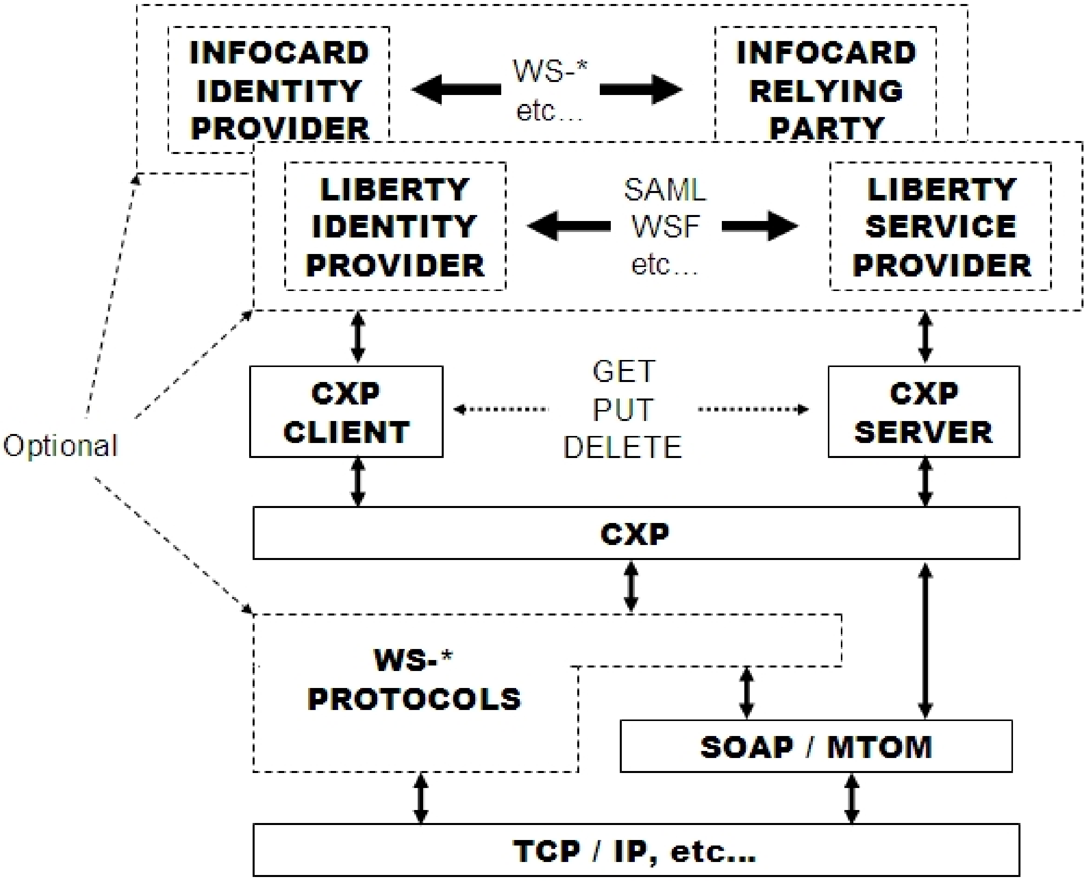


Thus, for example, the same CXP protocol is used between (a) the glucometer on Jane's belt and a network based Fictional Home Healthcare Hub service at http://fhhh.net and (b) the HealthStuff PHR used by Jane to access her personal healthcare account from her Liberty-Friendly HMO. In the first case, the trust relationship between the client and server is established by a PKI cert in Jane's glucometer, that is honored, or possibly issued, by the FHHH service. In the second case, the trust relationship is between Jane's IDP (her HMO) and the FHHH Service Provider via the bilateral Liberty Alliance business agreements.



Architecture

To achieve connectivity, each end of a CXP connection must support the same SOAP/MTOM/WS-* Protocol selection depending on the requirements of the federated identity management provider, if any.



There is a well defined and standard separation between CXP Clients and Servers; clients make requests, servers process requests and respond. Although nothing precludes a program from being both a CXP Client and Server, typically they have distinct roles within a distributed healthcare network. Normally, a CXP Server is the front door for a document repository and may also optionally interact with one or more registries behind the scenes.

CXP requires that each Client party initiating a transaction supply an opaque Sender identity token and that both parties maintain an audit log of each CXP transaction so that the logs of each party can be conjoined for forensic problem and dispute resolution. These tokens may be hardwired shared secrets, or otherwise obtained dynamically via methods outside CXP, as for example, from SAML or InfoCard.

Identity Federation

But it is more interesting to consider CXP when used in conjunction with a Federated Identity Service such as Liberty Alliance or Microsoft's InfoCard. In this case, the two parties establish a static trust relationship within the framework of the Federation Service, and dynamically use SAML2.0 and SOAP based WS-* to communicate CXP payloads.

The Client side initiator of a CXP transaction obtains an opaque Sender identity token from the Liberty or InfoCard IDP and passes it along to his counterpart (the Liberty Service Provider or InfoCard Relying Party) as above. But instead of hard coded secrets, or cumbersome certificates, the federation services permit dynamic interconnection of CXP participants who have signed bilateral business agreements and demonstrated technical compliance.

If a CXP Server is owned or otherwise associated with a Liberty Alliance Service Provider or InfoCard Relying Party, then that CXP Server can be exclusively available to only those CXP Clients whose Identity has been vetted by a trusted Identity Provider and has a pre-established bilateral trust relationship with the Service Provider/Relying Party. This allows not only for the federation of Identity outside of CXP itself, but allows small software and device vendors to benefit from the enhanced security and trust models of the Liberty and InfoCard.

Once a Identity Provider of any variety signs an agreement with a Liberty Alliance Service Provider or an InfoCard Relying Party and their technical infrastructures have been upgraded as necessary to support WS-* and SAML2.0 then the CXP Server can begin to offer services to the IDP users. If the Service Provider/Relying Party application presents a User Interface in addition to the CXP interface, then the single sign-on (SSO protocols) will likely be utilized between the service and the IDP, without regard to CXP. If the only protocol is CXP, then the WSF-2.0 protocols are utilized to allow secure and authenticated remote web service calls.

To support a network the size of the NHIN it will be necessary to run many CXP Servers in front of many repositories under a single Service Identity, In this case a single x509v3 Cert can be shared by the entire farm and WS-* redirection protocols may be utilized to put all of the servers under a single public name. The CXP client connects to the service and is transparently redirected to the appropriate server.

Alternatively, when the CXP Server is a Document Repository, and there is a separate Document Registry, the CXP transaction initiator (the document source) may choose to have an initial conversation (WSF2.0) with the Registry (e.g. a Liberty Service Provider or InfoCard Relying Party) to determine which Repository to contact. In this case there is an implied transfer of trust from the Registry to the Repository and the CXP protocol is then utilized as documented herein. When using a Federated Identity Service this initial conversation is mandatory and supplies the same opaque Sender identity token.

Registry Options

Finally – CXP may be used as a low-complexity, simple mechanism for document storage/retrieval from other types of registries and repositories. The use of multiple registry parameter blocks permits opt-in on the part of the call initiator to other repository models such as the ebXML-based IHE-XDS.

The leverage gained from federation by both identity providers and service providers towards the establishment of an NHIN are enormous. The identity providers can focus on membership, verification, and personalization. The service providers can focus on safe, cost effective healthcare.