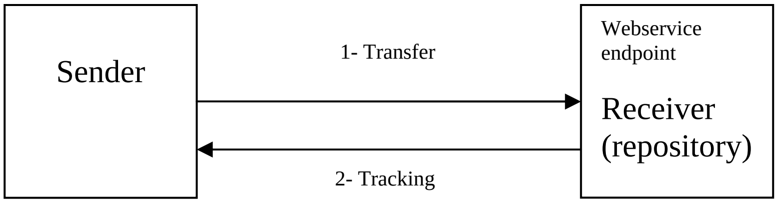
CCR Exchange Protocol (CXP)

CXP is a two party peer to peer protocol that moves CCR-family data and other XML based structures across the Internet between co-operating Sending and Receiving systems from multiple vendors. CCR-related data includes PDF, DICOM, and other documents referenced from within a CCR, and a CCR itself.

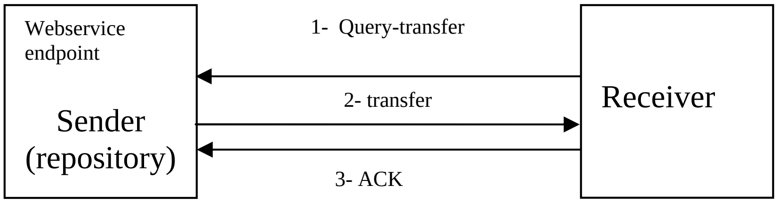
A Transfer is the movement of a CCR and Referenced documents or other XML based data. In CXP, we refer to whichever party is holding and moving the CCR as the Sender, and the party that is accepting and potentially storing the CCR as the Receiver.



1- ws call from Sender to Receiver
2- Receiver returns immediately with Tracking Number

Figure 1

A Transfer is initiated by a Transfer Command calling a pre-registered webservice endpoint URL. As shown in figure 1, a basic Transfer flows from Sender to Receiver, is safely stored by the Receiver, and a Tracking Number flows back from the Receiver to the Sender.



1 Receiver requests transfer with query params
2 ws call from Sender to Receiver
3 Receiver acknowledges receipt of query
4 optionally repeat for multiple items in query

Figure 2

CXP supports both Sender initiated and receiver initiated transfers, which we call Query-Transfers. As show in figure 2, Query-Transfer can return one or more CCRs and associated attachments.

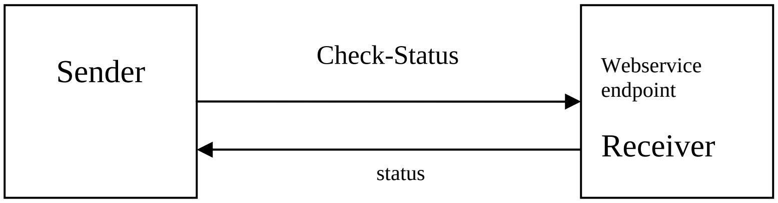
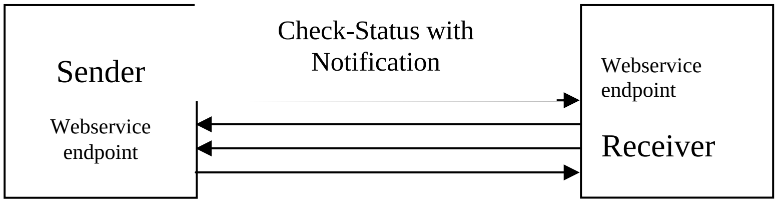


Figure 3

As shown in figure 3, the status of a particular CCR can be polled via a Check -Status Command. During the lifetime of a CCR a number of different statuses may be observed.



1 ws call to Receiver
2 Receiver returns immediate status
3 …. Receiver notifies Sender via ws call with XML Data
4 Sender acknowledges Receipt of notification

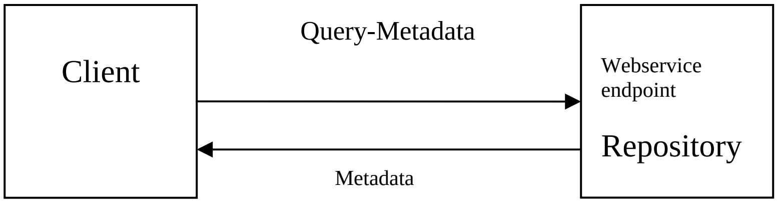
Figure 4

Rather than issuing periodic Check-Status Commands, an application may optionally supply an endpoint for CCR Notifications. As show in figure 4, this will invoke a pre-registered webservice endpoint URL whenever a status change occurs

Indexing and Retrievals

CCRs will be stored and indexed in different ways by different Vendors. There are no prescribed or mandatory keys, tags, or any identifying characteristics other than data present in the CCR itself and some vendors may accept CCRs alone, with no additional metadata. Vendors can index whatever elements of the CCR they choose and may accept an optional XML Data Block[1] to support the client authorization and query requirements when those elements are not accessible in the CCR.

Authenticated users and systems can locate a document in a repository and download a copy of the CCR-family data from the repository via the Query-Transfer Command with the repository as sender as shown in figure 2.



1 ws call to Repository
2 Repository return Metadata

Figure 5

[1] We may want to enter a constraint here that the XML block should not replicate data that is in the CCR. This is attractive because it means that there isn't the possibility of inconsistencies between the CCR and the XML block. It's unattractive because for some vendors the XML block may be condensed version of the CCR that parses more quickly or it may be some other standard XML format which requires (say) patient demographics. This should be nailed down by discussions with the accelerator group.

A Query-MetaData Command can be issued to retrieve metadata about CCRs. Different Vendors will support different Query options depending upon, security, and flexibility preferences.

The identifiers used in the queries (such as the tracking numbers specified above) are determined by the Receiver. Some may use UUIDs, others may use hashcodes, still others may have a simple counter. The scope of the identifier is determined by the repository – some identifiers may be permanent; others are time limited; still others may be one-time access keys. Defining these further is outside the scope of this proposal.

Interaction with Higher Level Protocols

There will be higher level protocols constructed on top of CXP. For example, there may be protocols for registration of Patients and other administrative tasks as well as for moving CCRs and attachments. In all cases these are layered on top of CXP as follows:

- CCRs and an optional XML-Data block are passed back and forth in standard form
- Administrative commands encode their functions and return status in an XML-Data block
- CCR Referenced documents may be transferred along with the CCR as XML-Data or separately by non-CXP methods.
- CCR References moving with the CCR are base-64 encoded and passed as part of XML-Data. This is the default. CCR References not moving with the CCR may need additional standards and protocols.
- SSL or TLS may be utilized and is encouraged between parties, but it is not required.
- Encrypted CCRs are permitted in CXP.

Thus the XML-Data block is where all non-CCR data that needs to be passed between systems is expressed. This is application specific.

Security

A CXP recipient vendor shall accept CCRs encrypted per the ASTM CCR spec. Status responses indicate if insufficient information was provided in order to issue a confirmation to the sender. In some cases, transfer of encrypted CCRs may require pre-registration of the patient or other Actors. These pre-registration steps are considered higher level protocols beyond CXP.

The CXP sender must accept responsibility for release of information to the recipient. Patient consent to information release is the responsibility of the sender.[2]. Consent and

[2] For example, use of a recipient's public key as derived from a consent form explicitly signed by the patient is one way to satisfy this legal mandate

the key management are outside of CXP. Another example might be implied consent between two CXP systems that have a HIPAA provider or business associate relationship and that authenticate each other via TLS. The HIPAA relationship is beyond CXP. Other consent mechanisms may exist, all outside CXP.

A CXP receiver is expected to manage its own security independent of the sender system or vendor. There is no defined responsibility for a recipient to publish general policies or to handle security for a particular transfer in a particular way. If the sender needs specific security information to manage its own policy, then the negotiation of these assertions is beyond the scope of CXP.

Apart from the use of SSL and TLS there is no authentication of the machine at the other end of the CXP connection. A Sender and Receiver can agree to use extra fields in the XML Data Block to pass additional authentication data such as a shared secret in order to provide additional validation to the transaction.

Implementation

CXP is based on SOAP over HTTP(S) or alternatively POST over HTTP(S). A Sender or Receiver may choose to implement either or both alternatives. This is a static choice made by the Vendor during installation. If implementing both, a separate set of URL endpoints will be utilized.

For a Sender to reliably connect and transfer a CCR to a Receiver, the Receiver must have a fixed public IP address and must publish the URL(s) (via email, word of mouth, etc) prior to accepting CXP connections.

A Sender does not need a fixed address but a Sender without a fixed public IP address is unable to receive notifications of Transfer status changes and will instead need to poll for this information[3]

For those operations such as Queries that do not imply a Sender and Receiver, but rather a Client and a Repository, the Repository is required to have a fixed IP address. If the Client has no fixed address, it is restricted to periodically re-polling the Repository and returning individual CCRs without attachments . If the Client has a fixed address, it can establish a URL which will be invoked whenever an incoming Transfer is available.

[3] We abandoned the notion of letting the receiver have a floating address and periodically poll for incoming CCRs. This implies buffering, queueing, and possibly databases on the Sender’s side. .

Commands

All commands map directly to SOAP or POST over HTTP. For compatibility, only a single output argument is utilized:

The general form is:

Xml-Return-Data = CXP-Command([CCR],[XML-Data]);

- ALL invocations of cxp-command return an XML data structure. The formats of this data structure are discussed below, and in the Errors section.

- Either the XML-Data block, OR the CCR must be present. Otherwise an encoded 404 error is returned to the caller.

- If the XML-Data block is absent, and operation-code of 'Transfer' is implicitly assumed. Otherwise the operation-code in the XML-Data block is utilized and other data values are defaulted as described elsewhere in this spec.

- Some operation codes return a real CCR as the XML-Return-Data, others will generate other XML return structures. This will evolve other time.

The same form of command is used in both directions. When a Notification of an incoming CCR is delivered via SOAP or POST, the argument list is exactly as described above.

Operation-code	**CCR**	**XML-Data Block**	**XML-Returned-Data-Block**
Transfer	Yes	Optional, if present includes notification URLs	Returns tracking number or error
Check-Status	No	Yes, includes tracking number	Current status of particular CCR
Query-Metadata	No	Yes, includes query params	Returns xml structure metadata about a collection of CCRs
Query-Transfer	No[4]	Yes, includes query params and notification URLs	Returns success or failure for query Invokes notification URL with an incoming Transfer

[4] If a Query returns a CCR plus attachments, then the simple form of Query can not be used to get the attachments. Instead, a notification endpoint is specified in the XML Data Block supplied with the Query. The endpoint will be called with the CCR and attachments encoded as a CCR and an XML Data Block that can be decomposed into separate attachments

Error Handling

Any invocation of CXP-command can return all O/S level TCP and HTTP errors. Beyond that, everything is returned as valid XML. All errors come back as valid XML structures.

XML-DATA

The XML-Data block passed between Sender and Receiver has different fields of interest depending on the specific operation request. The general structure, which is always unencrypted, is

```
<cxp:xml-data>
        <operation-code>opcode</operation-code>
        <fileset>
                <file>
                        <name>as-named-in-ccr</name>
                        <type>one of: pdf, dicom, etc </type>
                        <bits>base64-encoded-bits</bits>
                </file> …….
        </fileset>
        <sender-id>arbitrary sender id key returned with status </sender-id>
        <require-unique-ids>yes or no,
          depending on whether duplicate sender id keys should be rejected
        </require-unique-ids>
        <status-nofication-endpoint>
                <uri> https://mumbler.mumbler.mubler/mubler.xyz?data=foo</uri>
                <method>SOAP</method>
        </status-notification-endpoint>
        <query-nofication-endpoint>
                <uri> https://mumbler.mumbler.mubler/query.xyz?data=foo</uri>
                <method>POST</method>
        </query-notification-endpoint>
        <query-params>
                <querystring> tbd, and possibly vendor dependent </querystring>
        </query-params>
        <arbitrary-params>
                Bilaterally agreed xml snippets, possibly for authentication, billing, etc
        </arbitrary-params>
</cxp:xml-data>
```

The only mandatory field is operation-code. The other fields are present or not, depending on the needs of the operation-code. The xml data block is naturally extensible by adding additional tags which must be ignored if not understood by the Receiver.

Trademarks and Intellectual Property

CXP (or whatever the CCR Accelerator Group chooses to call this) is an alternative to XML File Import or Export from a Vendor System when the file is a CCR. CXP provides the alternative of a Web Service endpoint for the Import or Export target and, beyond that, offers the minimum required set of tracking and status protocols to enable reliable transfer of responsibility between two cooperating vendors. It will be useful for either ASTM or AAFP or the CCR Accelerator Group to take ownership and control of the trademark for Web transport via CXP in order to improve the rate of adoption in the marketplace.