# CDS Open Issues List

1. BCCampus typically sends a batch to a particular institution and uses a PSIS code as a WSDL element to identify the target institution. PESC is more likely to use something akin to the AcRecBatch which may contain multiple documents and targets where the institutional target’s identifier is included in the transmission header for each document. So we will need to decide what approach we will use and whether or not to use an institutional id at the WSDL batch level.
2. Batch size can be a factor for receiving institutions. We need to consider a size limit for received batches and some sort of flag indicating that more data is available.
3. Web service calls have security built in but BCCampus chose to also include username and password at the WSDL batch level. This might be advantageous in order to authorize server administration or reporting functions. The downside is that these credentials would need to be supported on the server.
4. BCCampus did not choose to include error messaging in the responses from the server and Jam suggests that it might be useful to include an xml structure to support error messages.
5. Jam pointed out that we’ll need to identify a host for the WSDL and any schemas and that the target namespace will need to be adjusted to this host.
6. How do we verify the sender so that we can trust the source?

*I pointed out that CDS would be a closed network and that we will be considering whether or not to include username and password within the WSDL interface.  I sense that they didn't feel that this was sufficient.*

o    We will need to figure out the participant provisioning strategy. Currently the sender can also be a receiver we haven’t dived deep enough to know if we need a rollup for institutitutions or vendors who are only

  Senders Only

  Receivers Only

  Sender and Receiver

o    Provisioning can happen on two basis

  In a closed network an administrator type of user configures the participant .

  This is the most simplest way to attack this problem.

  This does not cover any due diligence that needs to happen until the decision to provision a participant is made. The due diligence process will need to be discussed to address any concerns raised..

  In a open network – the participant have handshake to register to the open network . this implies any one can play here.

o    Securing the WSDL imply three levels

  Securing the transmission (SSL etc)

  Securing the payload (encryption like 509 certificates)

  Securing the session (this is where the credentials come into place  - some other forms are using special time sensitive tokens )

  Our initial proposal was to force users to authenticate and authorize a session for every service call.

o    If the team did not feel comfortable with this options then we would need detailed feedback on which areas are of a concern and what implementation strategy is of concern.  In addition, if they have concern then probably also have a possible solution so we can ask that as well.

1. How do we assure that the contents are not changed between the source and the destination?

*Documents will be encrypted but I couldn't fully respond to this because my understanding is that in order for the CDS processes to work they have to decrypt the package to get at the transmission header.  I think this is how the Texas server works currently.  Again I don't think this answer was fully satisfactory*

o    *This is the bottom line for the system – junk in junk out – stuff in stuff out.*

  *We are not anticipating to decrypt OR transform the data*

  *Unless we offer EDI to XML OR XML to EDI options or one standard to another standard options  on a payload this is applicable.*

o    *We ensure the integrity of the contents by ensuring that the transaction payload is secured in the transaction container (Request XML) – there are different ways to do this. We propose one way.*

o    *We can always have enough data in transmission header to capture details on the transaction. If PII (personally identifiable information) data is an concern here then all we can capture is that there was a transaction between a specific sender and the specific receiver – this data will need to be non encrypted OR we will need the CDS system to access it to ensure the delivery of the transaction (and the document(s)) in it to the intended recipient.*

o    *The reporting needs from CDS may affect some of the strategy here – for example if the reporting needs any PII data then their concern is valid.*

o    *We will need to understand what their exact concern is to reflect on the concern further as a* group.

1. Have we decided on SOAP or REST or will we support both?

*Typically PESC talks of SOAP but we haven't fully addressed this*

o    *PESC being a standards organization will probably never support one technology to other – be it SOAP vs. REST or XML vs EDI.*

  *Said that on this topic there are technologies like WCF that can support both SOAP or REST based api.*

  *There are pros and cons on both methodologies – we can bring this to the larger group to discuss which approach is more preferred.*

1. Do we include functionality for address verification (e.g. in the case that someone requires that a hardcopy be mailed)?

*No, but that could easily be included in the directory information that is reported out of the system.*

o    This will need us to subscribe to paid address verification services. [USPS API](https://www.usps.com/business/webtools-address-information.htm) may be a free one. Since this is meant to be an electronic solution we should ask the group if this aspect needs to be considered for a paper based clearing house functionality.

o    There are vendors in our group that do this today – for example parchment. We can ask the group to see if this service even makes sense to be part of CDS. Do we know if Parchment subscribe to a  service like this?

o    Just like the payment option – we can probably document and probably push  this to later phases.

1. Do we have a method to provide to verify to the sender that the document made it to the destination?

*No, so far we've only identified WSDL inputs/outputs.  Document level acknowledgments are typically handled by the document level protocols, e.g. TranscriptRequesAcknowledgement, with which the recipient institution ought to respond.  I'll add this to the*

This will certainly be handled – we did not get to that point yet.

1.      We can capture in CDS when the sender picked up the transaction(s)

2.      We can allow for an explicit web service call for sender to send an acknowledgement receipt back to the centralized system. The sender can poll this by transaction identifier in a batch fashion.