**Meeting/Call Notes - OpenHIE Interoperability Layer Community**

**Date**: 26 November 2013

**Attendees:**

Carl

Ryan

Hannes

Kari

Linda

Shahid

**Agenda:**

* ~~Discussion with Mulesoft about the work in the Philippines and how we can collaborate.~~ (The Mule guys canceled as something urgent came up)
* The interoperability layer work in RSA
* Authorization and authentication - restricting what endpoint certain users can access
* Vision mission and values and the implementation guide

**Call Recording file #**

**97444001**

**Meeting Notes:**

As both the Mule team and many of the Regenstrief team are unable to join due to urgent work taking priority, the agenda shifted to the work needed for the OpenHIM to meet current needs as driven by users, inc. within SA context.

*Security*

Must move away from self-signed certificates

Although we can authenticate we also need to have authentication to ensure system users can access only those channels they need but not other channels

Authorisation:

1. Core to IL

IL deals with end points - web service end points for various components - and we need to restrict access to these

2. within orchestrators

When an encounter is submitted (ID pf DR in message) has the authority to do this (only relevant to certain transactions)

Orchestrators should have the ability to check roles/permissions

SK - G3 application at Regenstrief does handle authorisation at provider level.

RC - Currently have an ALDAP database that allows any connection that supplies matching info to access (for system authentication not human users e.g. a clinic)

Could assign roles to those accounts within ALDAP database but may be too complex and have found this is a difficult process - may be better to store in a relational db or a NoSQL database

HV - ALDAP may be useful to some implementers but could provide option for other db

for legacy reasons?

CF - In low-resource settings what are possibilities of having existing ALDAP db containing all apps that may share data?

RC - Selected ALDAP initially because Mule ESB has features that plug into this easily

Agree simplifying it is a good idea but how to do within Mule ESB

Leads to another question: maybe should move away from Mule ESB as technology for the core

Disadvantages: it Is fairly static / not dynamic - not best suited to basic processes that should be configurable

Advantages: Orchestration and transformation (adaptors)

RC - Thinking we should maybe change core to another technology

SK - Mirth has moved away from Mule ESB as well

Have ver 1.0 as core using Mule ESB and then could we move to a version 1.x with a new, slimmer core

RC- Have already split the orch/mediators from the core

One of the main reasons to not having done end pioint security is the diff of doing it in Mule

HV - Would we define a role, link to user and see if should access end points

or

should we want to try and filter docs based on user role?

CF - Think of it like an excel spreadsheet (matrix) with user vs. end points

don’t think we need filters based on needs we have now

Remember we will not be the org who will be having to manage / administer the system on long-term basis - needs to be simple and easy as possible to administer while meeting requirmenst

Would like to be able to add system users

The next step would be to dynamically allow addition/creation of end points in a running HIM

This is offering **a very valuable service** to potential users : Can authorise, authenticate, log and manage errors

RC - Agree, filtering by doc type falls into same area as authentication of specific providers/ human users

SK - Big step up to Mirth 2.0 inc:

allows re-try of sending failed messages

strike data from messages and store as metadata within channel

is backward compatible

Added a lot of new functionality / better performance

Implemented it last week and still monitoring it (the free version)

SK - How do you propose having a secure connection from end point to HIM?

HV - client won’t be connecting - using http

issue we have is that self-signed certs being rejected by client libraries

CF - won’t be losing the SSL line to HIM , just wanting to use cert from Thawte,Verisign instead

CF - Can channels in Mirth be restricted to various users?

SK - think we can filter based on a tag - not sure if this can be used for authentication as well - could investigate

KS - When we looked at Mirth a lot of the security features were only available in the paid version

CF - There is a huge need for this and need to look as to how we can add this to the roadmap

*Vision, Mission and Values*

Need to provide a draft V,M,V early in the new year as well as an implementers’ guide

Let’s consider this and what we would like to include

RC - We can draft initial docs and send out for community to feedback for V,M,V

Imp guide is more of a challenge for now - should contain elements that are agnostic of technologies used eg: security implications for IL etc.

Can draft a table of contents for this

Jembi team can look at next week when all in CT

*Connectathon*

RC - work is on track and InfoMan is up behind the OpenHIM (infoman actor in IHE profile) and call active service finder

HV - Doing PR and FR validation using CSD- PR done and FR nearly done. Need to do more testing as have had some issues

HV - asked which list to raise issues on? RC - use the architecture list as has reps from all communities

Lynne creating test cases for CSD and should be 80% done by end of this month