# OpenHIE Interoperability Layer -Call Notes

**Meeting purpose:** Community Call for OpenHIE Interoperability Layer

**Date:** 18-02-2014

**Attendees:**

 Shahid Khokhar (Regenstrief)

 Derek Ritz

 Hannes

 Joan

 Linda

 Ryan

 Carl L

**Agenda:**

• Vision, Mission and Values

• Update on development work

• Authentication and authorization discussion

o For systems users

o For human users

Conference recording 54890101

Meeting recording link: http://www.conferenceplayback.com/stream/27007057/54890101.mp3

**Minutes:**

**Vision, Mission, Values**

Our community needs to deliver a V,M,V set by 31st March

LT asked community members to have a look at some initial ideas in the Google document and add comments / brain dump

https://docs.google.com/a/jembi.org/document/d/1SUFC1d7YL3FLCWPLHsC1Ox0GT4DVxJUU4vOKf7r8pLU/edit#

Then will set aside time on the next SHR and next IL call to discuss and will then revert to one text process

Update on development work

JHS working on some test scenarios with the CSIR and Meraka Institute

Authentication and authorization discussion

o For systems users

o For human users

**• Vision, Mission and Values**

LT: placed a link in the ether pad to a google doc done on the issue. Jembi team brainstormed for possible things to look at. We need to agree and deliver a document set of these ideas. This is an introduction to the doc LT will start an email discussion. This is for people to add ideas to and make comments on. There is a strong overlap of the two communities therefore we are looking at it together. It will be sent out on the email for discussion. Will be part of the next SHR and IL meetings.

DR: Are comments being sent to one person? LT: until the next call we will use the doc for comments thereafter we will revert to the other process.

**• Update on development work**

Update on the development work for the IL working on coming up with designs for HIM core components will be built using NodeJF. We have started adjacent work on the core component. Framework is being put in place. Will open it soon for people to see the work being done there.

RC: Next week a proposal to have a hackathon beteween Jembi and the CSIR will probably happen in Pretoria focus on developing the HIM and build features within that tool. Will be getting contributions from them and we will keep people informed.

 DR: Who will be working on it. CF: We are working with the Meraka group.

**• Authentication and authorization discussion**

How do we think of this for the two users, this came out of the architecture meeting, what approaches do we want to take when we talk about these two. System users is the first priority and after that human users

• **o For human users**

•  **o For systems users**

RC: Systems that want to connect to the HIE will need a way to authenticate and authorize, authenticate to confirm which clinic/centre it is and what authority do they have for functions within the HIE.

Two distinct pieces to this looking for identification, who is on the other end of the line and identify the node. May not be a one to one relationship with the system and a node. Comes from a node and an application in that node.

RC: was thinking of a node as an application need to consider what a definition of a node is, is it one identification per application or is it one per node.

we identify each application rather than the server.

HV: the login looks at the application itself on login level that is already happening.

HV: support the authentication on an application basis

CF mapped to an application not to a server

DR: The way you give it routines on an application by application basis we are giving access.

DR: giving a certificate to the server doesn't give a lot of control

RC: within the HIM app you want to create an easy user interface to make the policy phase easy. for new applications receiving a certificate on application

CL reinforce to have level authentication not worry about running IP addresses from mulitiple places

We will do authentication of applications. Appner (?) makes sense to be used here

We are trying to solidify the authentication within the HIM design and share it into the group, feeding into the dev work we are doing with the new node work and we will try out the concepts in this application to see how it works in practice.

DR: the policy issues are out of our scope but there is a lot of governance that goes around issues so that we can usefully inform MoH of what the policy issues are.

RC: possibly a page on the wiki for the policy requirements

DR: will do an initial indication of the policy issues that are needed. We need to have management control.

RC: The HIM will have to manage this process of who has access/keys and we could advise on the policy around this.

DR: Want to indicate to a hospital how to manage their networks and the use of the system and who has access

DR: RC can send an email and DR can respond. RC will send email with a wiki page attached.

**Authorization**

Once we know that the app is cleared for the system what channels do they have access to.

The OpenHIM as the core component doesn't understand message content the only way is looking at the path and allow certain authenticated systems to send messages through to a specific path

https://wiki.ohie.org/display/documents/CSD+Query+for+services

LT - Will add an issues list to the wiki

CL: we will have a list of apps that is allowed to operate in the system.

IL support can have orchestrators and adaption for certain processes. keep the openHIM core message agnostic and build an orchestrator that is CSD aware and use that or do we develop it into certain of the core component.

Have an access control list for each of the orchestrators, have a more high level authorization for each app

DR: better served by saying that in the absence of a restriction a transaction will be done. if we have explicit restrictions it may be less work

RC: perhaps be more cautious by using the allowed only approach to prevent all having access.

DR: if we make the mistake and permit access when we shouldn't then there may be a privacy issue but if we don't let clinicians know things then we would perhaps have caused more harm in the delivery of service.

If we saying that we restrict expect for specific authorisation then we protect privacy but a stoppage of information flow could be a greater impact

CL: we want to make the apps easy to use. default allow or default deny what we need is an easy interface for ease of use. we need a clear and easy way to follow their data protection policies

RC make it as easy as possible for them to manage.

DR what is in the IL is complimentary to what is done at the point of service.

RC: may be useful to use a concrete eg. of transaction that would have that restriction and use it as our requirements from a country perspective.

CL gave a Practical example of the updating of nursing credentials

RC: there may be a need for another work flow for the update facility it may help to enumerate the key differences

CL: will be documenting the workflows for the use cases and prioritise the update one

CL: There is overlap that makes it difficult to manage across all the systems that contain health worker information.

RC: From the architecture meeting the workflows have worked well to show things in a way that people can understand. Could we use for the common areas of the IL. They won't be specific but it will be a common workflow that has a view of security

We could come up with the common workflows or use the sequence type diagrams

DR: it could be useful to approach it in that way, as the IL community we can document this is how we will be doing things in the IL 'Clear box'

RC: We could use the wiki pages as a base to capture these kinds of documents. Could be specialised workflows for the IL around authentication and authorization.

CL: may be useful to get sub community workflows

RC: perhaps cross cutting workflows and then sub community specific.

Take back to the architecture group and say this is the approach we are thinking of taking.

DR: natural groupings of profiles and have them together

CL: request for high level info he can use to introduce the HIM to Nigeria. RC will send information that he has that could assist.

RC will structure workflows for security processes