**Comments and Suggested Revisions**

**Towards the Architecture Section**

**of the 802.22.3 Standard Draft v1.0**

*Nilesh Khambekar*

Date: March 4th, 2017 [Comment version 1.0 ]

* + 1. Comments

Following are the comments on SCOS Architecture described in Section 5 of the standard version 1.0.

1. SCOS Architecture should specify high-level overview of SCOS-subsystems, SCOS users, and SCOS operational procedures .
2. SCOS Architecture should provide high level overview of working of the SCOS components.
3. Suggested name Sensing Data Manager for Data Push Service.
	* 1. Suggestions

Following draft attempts to address the above mentioned comments on the standard draft v1.0 references section.

Note: This document is being revised. Todo items are identified with [#ToDoText].

1. SCOS Platform Architecture
	1. Overview

The SCOS platform offers spectrum sensing as a service to its users. The SCOS platform users are called Actors. The Actors issue sensing request to the SCOS platform. The sensing data for the sensing request is disseminated to Data Receive Point (DRP).

Figure 1 illustrates the architecture of SCOS system. The SCOS platform comprises of three sub-systems: Spectrum Sensing Devices (SSDs), Spectrum Sensing Manager (SSM), and Spectrum Data Manager (SDM). SSM manages multiple spectrum sensing requests and creates sensing tasks for the SSDs. The SSDs perform the assigned sensing tasks and transmit the sensing data to the SDM.



Figure 1: SCOS system block diagram. [#ReviseDiagram]

* Actor is the entity that initiates a spectrum monitoring request to one or more Spectrum Sensing Managers (SSM). Actors can be human or machine, and have various levels of privileges regarding what spectrum information collection can be initiated. Actors specify the DRP(s) to which sensing data for a sensing task.
	+ An Actor (user of the SCOS system) and SSM (Sensing Manager) communicate by REST API to ask for available resources, and request a scan. [#Remove]
* Data Receive Point collects the spectrum information from the SCOS system. DRPs can be databases storing the data or machines processing the data to trigger client specific workflows.
* The sensing data is identified with a sensing request issued from an Actor.
	+ The Actor and DRP(s) for a sensing task may or may not be owned by the same organization. The data collected by a DRP is owned by the owner of the DRP. Authorization to access that data would rest with the owner of that data storage entity. and what spectrum information can be accessed from a Data Store. [#Revise #Move2DataOwnership]
	+ The DRPs can be, but not necessarily, associated with a specific Actor. [#Move2DataOwnership]
* The Data Put Manager transmits data to the Data Store via a Message Queue, and the Actor interacts with the Data Store using their chosen mechanisms (out of scope of this standard) [#Move2Messaging].
* Spectrum Sensing Manager manages a group of Spectrum Sensing Devices (SSD). SSM maintains a list of available resources at each SSD. SSM manages the usage of SSD resources and sensing schedules as defined by the policies for SSM and Actors associated with each sensing requests.
	+ The SSM is associated with SSDs (Sensing Devices) through a synchronous interface. [#Move2ArchMessaging]
	+ Requests for spectrum measurements from Actors are inserted into a scan schedule on the SSM for all its attached SSDs, as far as possible under a set of slot availability rules. This schedule is synched to the appropriate SSDs associated with the SSM. [#Move2ArchEntityFunctions]
	+ The SSM stores and manages a schedule of scans against the sensing resources, and synchronizes this schedule with all SSDs both on a change being made and periodically to ensure correct state. [#Move2ArchMessaging]
* Sensing Data Manager receives sensing data from SSDs. It maintains asynchronous interface with SSDs. SDM performs system data validation (i.e. that a transmission is received completely, partial scans are consolidated, etc). SDM transmits the sensing data to one or more DRPs as defined by the policies associated with each Actor (source of scan requests).
* Typically (but not necessarily) the SSM and SDM would be running on the same physical server.
* Spectrum Sensing Device is the sensing hardware that collects the spectrum data requested by the SSM on behalf of each Actor. The SSDs may exist with various levels of sophistication. The less sophisticated might be capable of measuring only one band, at only one resolution with little on-board processing. Other sensors may incorporate sophisticated antenna techniques, multiple bands, calibration processes, on-board data processing and/or storage and/or be capable of mobile operation.
	+ An SSD performs the scans in the schedule, and transmits the data and associated metadata through an asynchronous interface (message queue, or real time stream) to a SDM.
* Data Put Manager receives transmissions of packaged scan data from SSDs, and retransmits it to one or more destinations, as defined by the policies associated with each Actor (source of scan requests)
	+ The “Data Put Manager” applies any policies and then handles the Store & Forward to one or more data stores using a Message Queue or Streaming Mechanism
	+ Typically (but not necessarily) the SSM and Data Put Manager would be running on the same physical server.
* SCOS system may include SSM Proxies. An SSM Proxy lets one SSM talk to another, with the downstream SSM appearing as if it were an SSD with a set of resources it provides. This downstream SCOS system would need to be 802.22.3 compliant.
* SCOS system may include SSD Proxies. An SSD Proxy lets an SSM talk to any other proprietary sensing hardware, acting as a software translation mechanism that translates between commands/metrics/etc. It would need to be custom written for the particular device it talks to.
	1. SCOS Functional Block Diagram

The flow of instructions and data is described in Figure 3: SCOS Functional Block Diagram.



Figure 2: SCOS Functional Block Diagram [#Revise for SDM, DRP]

This diagram can be extended with the concept of proxying to allow SCOS systems to be cascaded, or the use of non 802.22.3 compliant sensing devices.



Figure 3: SSD Proxy

****

Figure 4: SSM Proxy

* 1. SCOS Operational Procedures

Figure 5 shows interaction between SCOS architectural entities.



Figure 5: SCOS Interaction Model

The communication between each of the entities defined above can be grouped and defined within the Interface Categories shown in Figure 6. Message Sequence and described below.



Figure 6. Message Sequence

* + 1. SCOS entity interactions
			1. USER <−> SSM
				1. Authentication and Registration

These procedures define the association and authentication process for an SSM and USER entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once an SSM is authenticated and registered to a USER, the USER can then discover the capabilities of the SSM and its associated SSD’s. The USER may then define and make sensing requests to the SSM, which include a designation of the DBstore(s) to which the data is to be sent. The SSM will notify the USER when measurements are successfully completed (or not) and available at the DBstore.

* + - * 1. Resource Discovery

Resource Discovery is the process of informing the USER of what capabilities that the SSM has with regard to what types of measurements, what bands can be measured and associated measurement parameters that can be specified and controlled and over what locations. This takes the form of a resource/capability descriptor and the current scan schedule per SSD.

* + - * 1. Scan Request

The Scan Request message from the USER to the SSM includes the parameters of the desired spectrum measurement to be made and any associated processing to be performed by either the SSD or the SSM. This scan request is wrapped in a scheduling task description, defining the time the scan is to be made, the repetition rate (if applicable), the locations, etc. When the scan parameters in their scheduling wrapper are received by the SSM it will be validated as possible to be executed (i.e. the resources requested meet the SSMs schedule of resources available), and either acknowledged as being queue, or a refusal is returned to the USER. If a scan schedule is upated for a particular SSD, it is then replicated down to that SSD.

* + - 1. SSM <−> SSD
				1. Authentication and Registration

These procedures define the association and authentication process for an SSD and SSM entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once an SSD is authenticated and registered to a SSM, the SSM can then discover the capabilities of the SSD. An SSM will have associated with it at least one SSD. The SSM may then assign sensing requests to the appropriate set of SSDs in order to fulfill the sensing request of the USER.

* + - * 1. Status and Discovery

The Status and Discovery process serves two functions. The first is to inform the SSM of what capabilities that the SSD has with regard to what types of measurements, what bands can be measured and associated measurement facilities (such calibration, antenna control, mobility, storage, processing) that can be specified and controlled and over what locations. The SSD will transmit a package describing its capabilities and available resources at time of authentication/discovery, and if there is any change in its configuration. The second function is to maintain association with the SSM. It will transmit a period heartbeat to indicate it is still associated with the SSM. If it is to disconnect, it will transmit a disassociation message (e.g. if it is rebooting or about to go into an offline mode).

* + - * 1. Scan Request

The Scan Request message originating from the SSM is sent to the appropriate SSDs for execution as a scan schedule. It includes the parameters of the desired spectrum measurement to be made based on knowledge of the SSD’s capabilities. This request will include the time to make the measurement, the repetition rate (if applicable), the locations, etc. and the format of the measured data. In the case of a single, once-off scan, the schedule will indicate no repitition.

* + - 1. Data Store <−> USER
				1. Authentication and Registration

These procedures define the association and authentication process for a Data Store and Actor entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once a Data Store is authenticated and registered to an Actor, the Actor is then authorized to cause data to be delivered to the Data Store, and read that data.

* + - * 1. Resource Discovery

Resource Discovery is the process of informing the Actor of what capabilities that the Data Store has with regard to what types of data can be stored, at what rate, at what access level, and in what quantity can be specified. It may also initiate that association of a particular Data Store with a specific SSM that will be providing the data.

* + - 1. SSM <−> Data Store
				1. Authentication and Registration

These procedures define the association and authentication process for a Data Store and SSM entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once a Data Store is authenticated and registered with a SSM, the SSM is then authorized to cause data to be delivered to the Data Store based on the privileges of the Data Store and the SSM. The Data Stores can be grouped into Data Store Groups, where a transmission of data from the SSM is delivered to multiple Data Stores.

* + - 1. SDM <-> DRP

These procedures define and enable the storage of data from the SDM to the DRP. The successful reception of this data initiates a notification of the initiating USER that requested that data.