# NSI meeting @ NORDUnet conference, Uppsala

***Attendees:***

Guy R.

Tomohiro K.

Tangui C.

Henrik T.J.

Joyce W.

John M.

Chin G.

Ralph K.

Freek D.

Diederik V.

Miroslav Z.

Inder M.

Hans T.

***Agenda:***

The meeting agenda can be found here: <https://redmine.ogf.org/dmsf_files/13348>

All presentations given at this meeting are available to download here: <https://redmine.ogf.org/dmsf/nsi-wg?folder_id=6596>

All draft standards and informational documents are available to download here:  
<https://redmine.ogf.org/dmsf/nsi-wg?folder_id=6526>

***NSA description (John M.)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13357>

* Document providing information relating to an NSI Agent.
* Describes the control plane topology (NSA peerings)
* ‘PeersWith’ reflects the trust relationship. Bidirectional, but in practice RA/AG/PA roles as defined in the ‘feature’ attribute will determine which direction messages can be passed.
* AG role implies that your NSA is committed to passing NSI messages to child NSAs.

Discussion:

* Is there a need to model an AG that behaves differently depending on who it is peering with? I.e behaves as an AG to some and as a PA to others.
* **AP1:** John to summarise on whether there is a need to allow an AG to behave differently depending on who it is peering with. Document and send to list for discussion.
* Three dynamic circuit service developers are coding an NSA description document as it is currently defined.
* The NSI working group agrees to submit the NSA description to public comment.
* **AP2:** John to tidy up NSA description document and submit for public comment.

***AAI (Hans T.)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13347>

Requirement:

* Every NSA in a chain must able to trace back an NSI request to the originating NSA and user.
* The entire trace is not needed.
* Authorization attributes must be transparently transported over control plane.
* Intermediate NSAs are allowed to add authorization attributes to a message.
* Subsequent modify messages also must be authorized.

Connection trace:

* Ordered list of NSAs that have transited the network.
* Two types of AG: the standard type will pass through the globalConnectionId and add the NSA to the connectionTrace.
* The ‘superAG’ will take responsibility as the originator of the Connection request. In this case they create a new globlaConnectionId and clear the connectionTrace. This is not allowed in the NSI standards, so is no-standard behaviour.

Discussion:

* Chin: Need a way of knowing who is taking responsibility for the authentication credentials.
* Proposal: message should include both the credential being used and the NSA who is responsible for the credentials.
* Miroslav: I would not like to allow re-writing of attributes.
* Proposal: Should the schema be changed to now include a security attribute list instead of a single security attribute. The list includes both and identifiers an associated NSA. This is not an ordered list – the trace is responsible for this.
* Proposal: move the connection trace out of the AAI requirement and into somewhere else?
* **AP3**: John/Hans to review the connection traceId and security attribute list proposals and come up with an agreement and update the document.
* Decision: The NSI working group accepts the proposed AA methodology presented by Hans. A detailed proposal AA to be documented and reviewed by the working group.

***Switching service and adaptations (John M.)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13361>

* Existing service domain concept: An STP can be connected to any other STP within a service domain.
* John presented switching service schema, Label swapping, hasPorts etc…
* Switching service only connects ports of same technology/label type so does not do adaptation… needs adaptation function.
* Switching service used to describe legacy native Ethernet, in particular its inability to re-use vlanIds.
* Adaptations allow service domains of differing technology types to be connected together.
* Currently interop testing is happening between ESnet, AutoBAHN, Surfnet BoD in Netherlight using the switching and adaptation functions.
* Decision: the NSI working group confirmed that the NSI switching and adaptation concepts as proposed should be included in the ‘NSI extensions to NML’ standard. Final approval of this standard pending completion of the document.
* **AP4**: A document is needed that describes how to create a service definition – this was dropped out of CS document.

***STP\_Ids (John M.)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13358>

* John summarized the different STPId proposals.
* New compromise proposal has been proposed by Chin with the following characteristics.
* Network has two parts a network and local-network part  
   i.e <networkID> = <network>:<networkLocal>
* The <network> portion has a year portion too, i.e. <network> = urn:ogf:network:[example.net:2014](http://example.net:2014)
* No colons allowed in <networkLocal>. Colons allowed in localId.
* <network> = urn:ogf:network:example.net: (note last colon is part of network Id)
* <networkLocal> = string without a colon allowed
* If networkLocal does not exist then = urn:ogf:network:example.net::<stpLocal>
* Decision: Chin proposal has been accepted by the working group.
* **AP5**: John to update NSI extension to NML with the Chin STPiD.

***Pathfinding requirements (Chin G.)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13345>

* Ran through the pathfinding requirements slide set.
* No requirement for congruency between control and data plane
* Message workflow can arbitrary.
* Sparse connectivity between NSA … may need to send request via 3rd party NSA.
* AG that is not directly managing resources is allowed.
* Request should be able to be issued anywhere (not just source based routing).

***NSI policy requirements (Henrik TJ, Hans T, Chin G, Guy R)***

Henrik: NORDUNet Policy

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13351>

* Restricted transit depending on user
* Restrict connection depending on domains involved in the dataplane path

Hans: Surfnet policy

* Currently no transit limitation
* Currently no local policy to authenticate the originating user
* Currently no some ports are policy free by agreement
* Currently need to know originating user/organization and the route by which it arrived at Surfnet.
* In future want to apply transit based local domain policy.
* In future want to have the ability to apply policies on transit traffic and other

Chin:

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13350>

* Transit – one end of a circuit must end a customer site (no transit)
* Example research transit.
* Policy applied at the circuit endpoints (transitive trust).

Guy:

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13354>

* In the BoD service AA is performed at circuit end-points based on the policies of the local domain.
* Transit traffic is accepted by default if a request comes from a trusted peering network (transitive trust).

***Policy requirements in NSI***

The NSI WG agreed that the following information is needed in a connection request to be able to apply policy:

1. Original (uRA) source and destination STP
2. NSA and user Id of the requester
3. Computed dataplane path (for chain up to that point)

***Overview of range of variants on types of distribution mechanisms (Freek D.)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13355>

* Freek provided the group with a good overview of the range of options for topology distribution and the pros and cons of each.

***Path vector routing (Henrik)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13352>

* NSA pulls topology info from peers and then updates reachability vectors
* Can manipulate vectors to influence preferences
* Currently same vectors per peer… ideally different vectors for each peer.
* Does not work well with exchange points
* Removes the need for topology distribution.
* Easy to implement – as little as 100 lines of code to implement.
* Problem: Does not support tree model

John: currently NSI does not support mixed tree and chain in the same connection. Should we add something to NSI to indicate if a tree or chain type workflow will be used?

***Document distribution Service (John)***

The full presentation is available to download here: <https://redmine.ogf.org/dmsf_files/13359>

* Distribution follows control plane
* Supports many types of documents: NSA description, topology, service definitions and policy documents.
* Peer-to-peer document flooding service
* Polling and subscription based notification
* Meta data: source NSA, type of doc, id, version, expires, signature
* REST based subscription.
* Operations: getDoc, addDoc, updateDoc, addSubscr, editSubscr, deleteSubscr etc.
* No path computation and policy implied.

***UvA topology distribution proposal (Ralph)***

The full presentation is available to download here:<https://redmine.ogf.org/dmsf_files/13349>

* Similar to DDS but focuses on topology only.
* Floods URL rather than whole document.
* Allows policy to be applied by on information distribution based on requestor credentials.

***Topology distribution and path-finding discussion***

* Glambda, OSCARS, Surfnet BoD all support tree model.
* GÉANT BoD uses chain model internally but can support an aggregator mode.
* OpenNSA does not support tree mode.
* Decision: Group generally agreed that non-congruency between data and control plane has been a feature of the GLIF implementation and will be needed in the future.
* Group agreed to support global interoperability OpenNSA will need a proxy function to convert incoming tree request to a chain. This is not an ideal solution.
* **AP6:** A team to be created to investigate mixed tree/chain modes and if these should be supported.

***Summary of action points:***

* **AP1:** John to summarise on whether there is a need to allow an AG to behave differently depending on who it is peering with. Document and send to list for discussion.
* **AP2:** John to tidy up NSA description document and submit for public comment.
* **AP3**: John/Hans to review the connection traceId and security attribute list proposals and come up with an agreement and update the document.
* **AP4**: A document is needed that describes how to create a service definition – this was dropped out of CS document.
* **AP5**: John to update NSI extension to NML with the Chin STPiD.
* **AP6:** A team to be created to investigate mixed tree/chain modes and if these should be supported.