# NSI v2.0: Agreed Features

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Topic** | **Proposer** | **Decision point** | **Include in 2.0? Decision** | **Benefits** | **Risks** |
| State Machine | CG | Do we need to solve the wait-for-provisioning confirmed problem? | Yes\* | TK: This is issue of how we model NRM in NSI architecture |   |
| State Machine  | TK | Should we split the state-machine in to withNMR and withoutNRM state-machines? | yes \* |   |   |
| State Machine | TK | Should we support Message Delivery Layer? | yes \* |   |   |
| State Machine | TK | Should we have '-ing' states? | yes \* |   |  |
| Aggregation | IM | Do we need a summarization/aggregation function? | yes \* |   |   |
| Error handling | HJT | Do we need a mechanism/policy to handle down-stream errors in the case of different errors from different children? | yes \* | Nested errors make better error handling possible. Makes it possible to see what actually goes wrong.  Helpful in path finding to know which resources need to be removed from the next request. | Higher complexity. Can get error codes for unknown NSAs |
| Error handling | HJT | Should we add an error code hierarchy -  group errors in classes: connection error, security error, topology error, internal error… | Yes \* | Easier readability. |   |
| Error handling | HJT | Should we change the WSDL to add NSA id to the error code - note this is an optional attribute. | Yes \* | Will permit requester to identify the NSA(s) that failed the request.   | Requester NSA might not know about the NSA generating the error.  The NSA hiding the existence of the NSA generating the error can remove it’s ID from the list and add it’s own. |
| Error handling | TK | Should we classify errors as: recoverable and unrecoverable errors. | Yes \* | For the purposes of defining error recovery mechanisms, we should be clear about which errors are recoverable. |   |
| Protocol versioning | JM | Protocol versioning using SOAP, WSDL XML namespaces | Yes \* | Already done. |   |
| Version discovery | JM | NSI should define a simple web service for NS interface protocol version discovery | Yes \* | Group will work through an appropriate definition.  Action to investigate  into DCN defined mechanism. |   |
| WSDL | JM | Proposal – move header information from body into SOAP header.  This would include: correlationId, replyTo, reqNSA, provNSA | yes \* | Simplifies compiler generated and simplifies WSDL definitions. |   |
| EROs | IM/ CG | Should we support EROs? | yes \* | With the agreement to expose internal topologies and manage sub-networks. Also with the intention of this protocol being used by network administrators, constraining the path with intermediate points is essential functionality | NONE |
| Topology | JS | Support unidirectional connections as request option? | Yes \* |   |   |
| Topology | JS | STP Type value pairs:  should STP bundles supported? | yes \* |   |   |
| Topology | JS | Should we define a common way to map STPs to NML and 'maps-to' to underlying NML? Note: SDP is a mapping between STPs, so it conceptual and has no identifier in NML. | Yes \* |   |   |
| Topology | TM | Should we support the commercial requirement (#2) data model should be independent of underlying network technology: PBB, EoMPLS,  | Yes \* |   |   |
| Topology | many | Should we support definition and advertisement of domain-internal topology? | Yes \* | Domain internal topology will utilize NML to model links and nodes. |   |
| Topology service | IM | Do we need a topology service?  How would this be implemented? | yes \* | Make the service self-contained. Makes dynamic topology updates possible | The topology service can be exchange huge amount of data because of FQ-STPs. Need summarization or aggregation functions |
| Topology service | JS | Do we need an inter-network topology exchange mechanism? | Yes \* |   |   |
| Topology service | TK | Do we need to have a mechanism to represent and advertise network internal topology?Note: but advertisement mechanism is out of scope for NSI-CS protocol. In-scope for NSI framework | yes \* | STP provide the higher level service abstraction on the network edges, while the internal network topology is modelled using NML links and nodes. | We need to avoid abstraction upon abstraction which this should avoid. |
| Topology service |  |  |  |  |  |
| Topology service | IM | Do we need a process/method for to resolve control plane reachability? | Yes \* | Without this, none of the above features will work. NSA pathfinding is important to do to effectively request (in tree mode or tunnelling) services from those domains | Are there any security risks in advertising the trust topology? |
| Firewall | JM/HTJ | Should we make NSI more NAT/firewall friendly sometime in the future? | yes \* | Agreed to prototype a simplified firewall safe protocol for end users and simple requester-only NSA.  May be used for NSA-to-NSA communications if proof of concepts proves viable as a solution. | Need to make sure new behaviors of protocol does not impact NSA message throughput. |
| Firewall | JM | Should we require that provider NSAs be publicly accessible through the firewall in v2.0 | yes \* | Decision was they need to be publicly accessible. | We are investigating firewall safe access methods. |
| Service Definitions | JS | Is the concept of an SD a requirement for NSI | Yes \* |   |   |
| Service Definitions | JS | Are tech specific attributes in connection request required? | yes \* |   |   |
| Security  | IM | Should security be based on TLS/SSL and/or WS-Security? | Unless we get a better proposal this will be accepted  | TLS/SSL for message transport encryption. Mutual authentication for non-NSA client identities that translate into authentication. WS-Security for authz with tokens and attributes.  | WS-Security toolset is not uniformly supported for development kits. Implementers need to make wise choices. |
| Security | IM | Authorization using SAML attributes? | Unless we get a better proposal this will be accepted  | Security world has blessed this approach and using it for different applications. TK: This is “a” security profile. | None |
| Security | CG | Do we need an alternative authorization mechanism?  | Unless we get a better proposal this will be accepted  | TK - alternative ‘security profiles’ should be possible? |   |
| Security | IM | Should we add policy: NSA **must** add its attributes and **should** forward upstream attributes?TK: forwarding should be done according to policy of requester and NSAs. | Unless we get a better proposal this will be accepted  | These seem to be the minimum required of must’s and should’s for the protocol to work.  | Best Practices might require MUSTs for both, or some networks may require it. That is fine and consistent with the protocol.  |
| Security | IM | Should we have common SAML attributes: essential: Name, project, institution, Other attributes are optional  | Unless we get a better proposal this will be accepted  | Having common standard attributes covers 80% of the cases hopefully.  | There are mechanisms to cover the other 20% of cases. Since those are handled in pairwise basis, it should not put risk on the protocol at all.  |
| Security | IM | Should SAML have two fields: Ultimate requester credentials and requesting NSA credentials. Either one can be empty, but both should not be | Unless we get a better proposal this will be accepted  |   |   |
| Security | IM | Trust: delegation of trust required if user detail have not been passed on | Unless we get a better proposal this will be accepted  | There is no other way authorization can happen. | we still need to handle the case when attribute substitution happens |
| Security | IM | Decision: Decouple the transport security from the Authentication?  | Unless we get a better proposal this will be accepted  | Rationale was to make the protocol not dependent on transport layer security for auth, encry or integrity of the messages | Requires more dependence on WS-Security and getting rid of TLS/SSL. Needs more discussion. |
| Security | IM | Support 3 WS token mechanisms | Unless we get a better proposal this will be accepted  | Most flexible that supports dev/test environment, legacy certificates and most popular approaches of today | Configuration needed to make sure there is knowledge on what subset (if any) does the NSA support |

# NSI v2.0: Dropped Features

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **Proposer** | **Decision point** | **Include in 2.0? Decision** | **Benefits** | **Risks** |
| Simplification  | JM | For simplification of the NSI protocol, do we require congruency between data plane and control plane?  | No \* | Simpler breakout of reservation and makes chaining possible. | Probably won’t match real world. |
| Simplification | JM | For simplification of the NSI protocol, do we use NSI to tunnel reservation request be sent to head-end NSA before processing? | No \* | This allows users/NSA remote from the source endpoint network to issue a chain request to source endpoint’s  NSA. | Need to introduce new signalling plane message tunnelling /routing feature.  |
| Simplification | JM/ IM | For simplification of the NSI protocol, do we remove support for the tree model, and do chain model only? | No \* | Permits only one mode of routing, and with #1, will not require reservations on NSA not in the data plane path. | If we can’t assume #1 then we can’t support chain only. |
| Simplification | JM | For simplification of the NSI protocol, should we by policy require the ultimate requester to send a connection request to head-end NSA only? | No \* | Argument is that if the end user has permission to utilize the resource in the head-end network then they should be able to talk directly to the head-end NSA to request the reservation. | Although may remove reservation state machines from some NSA that are not involved in the data plane, without #1 to permit chaining to data plane only NSA, then this does not provide value. |
| Topology  | JS | Should we re-define NSI topology to be based unidirectional STPs. (2 requests to create bidirectional connections) | No \* | method for mapping to unidirectional concept in NML needs to be proposed |   |
| Service type | TM | Should we support the commercial requirement (#1) for requests for point-to-multipoint networks. | No \* | NSI will be used by commercial network in the future. For commercial network, the multipoint network is essential. |   |

# NSI v2.0: Features pending agreement

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **Proposer** | **Decision point** | **Include in 2.0? Decision** | **Benefits** | **Risks** |
| Topology service | IM | Should NSAs advertise their control plane trust topology, or whole topology? | ? |   |   |
| Error handling | HJT | Do we need a separate set of downstream error codes… other solutions? | ? see item 15 AP |   |   |
| Topology  | JS | Should we add a rule that an SDP (pair of STPs) has an 'inside-STP' and 'outside-STP' defined? Motivation: this will allow us to add conventions to help with pathfinding problem | No? |   |   |
| Topology | JS | Should we add conventions to ensure consistency of path-finding. So where an STP is selected as a path end-point, the connection should be built on the 'inside' direction? | No? | helps make pathfinding un-ambiguous |   |
| Query | TK | Do we need an ‘availability query’? | ? |   |   |
| Firewall  | JM/HTJ | Make NSI more NAT/firewall friendly in NSI v2.0? | ? |   |   |
| Firewall | PB | Should the client NSA be publicly accessible? | ? |   |   |
| Firewall | TM | Should we support the commercial requirement (#3) NAT aware interface.  I.e should support non-persistent client requester Agent | see issue 33 |   | Why add this as a ‘commercial requirement’ as it is already a known problem. |
| Notification  | HTJ | Which strategy for state updates? |   | (depends on protocol choice) |   |
| NSI client | JM | Should a separate NSI client be defined? | ? | APs will provide investigation towards a simplified interface for clients. | “NSI client” is insufficiently defined. Will it have a smaller state machine? If the client interface does not expose the full NSI functionality, then clients become completely dependent on pathfinding etc., which is not yet defined. |
| Topology  | JS | Should we use hierarchical networks in topology to express domain internal topology? | no? |   | We previously stated that only a single NSA can manage a network, however, allowing this means we now have multiple NSA managing a single network (although they could be proper subsets). |
| Topology | JS | Should aliases be added to NSI topology? | no? |   |   |
| Topology | TK | Internal topology proposal:  domain internal topology is represented using NML with a relationship between SDPs with NML edge ports |   |   |   |
| Pathfinding  | TK | Should it be possible to select any STP as an end point?   |   |   |   |
| Pathfinding | TK | Should we define how to interpret ingress/egress STP when path finding? |   |   |   |
| Pathfinding | CG | Should we allow end-networks with no transit to impose policy on a path request? | Yes ? |   |   |
| Pathfinding | CG | Should we add optional constraints to NSI v2.0? | ? | Maybe able to leverage sessionAttributes | To be investigated |
| Service Definition | JS | Should end-point details be included in service definitions? Eg STPs, end point VLANs etc? | ? |   |   |
| Service Definition | TK | Proposal: ‘candidate STPs’ are described in the topology and are used in connection requests.  The connection confirmation return ‘STP instance’ |   |   |   |
| Service Definition | JS | Should SD defaults be available for use for path-finding?  | ? |   |   |
| Service Definition | JS | Should SD reflect network’s performance or performance of lowest common denominator service? Proposal: 2 types of SD: common and network specific. | ? |   |   |
| Service Definition | JS | Should SD be available on web? i.e. - provider can announce URL of SD.  | no? |   |   |
| Service Definition | JS | Should SD be part of the NSI version service proposed by John M.? | yes? |   |   |
| Service Definition | JS | Should access to SD be subject to authentication?  | ? |   |   |

# NSI v2.0: Actions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Proposer** | **Action point** | **Benefits** | **Risks** |
| Error handling | HJT | HJT to prepare a short description of which errors are recoverable and which are not recoverable. |   |   |
| NSI client | JM | John M. to prototype a light weight NSI client |   |   |
| NSI client | JM | John M. to produce a list of NSI functions that are mandatory for NSI client |   |   |
| Firewall | HJT | NAT/firewall: Do we switch away from call backs? | Makes clients simpler to build and use | Wasted time on creating & implementing protocol |
| 23 | HJT | Henrik to prepare proposal to solve this issue:  Should we propagate, abstract, list?  |   |   |
| Topology  | JvdH | Jeroen:prepare XML representation to relate STPs to NML. |   |   |
| Topology | TK | Propose a syntax for announcing STP pairings |   |   |
| Policy Documentation | GR | Guy to document that edge networks that have no NSA can have a conceptual STP, however since these are not announced, they will not exist in the topology |   |   |
| p2mp | TM | Prepare a proposal on how point-to-multipoint could be implemented in NSI |   |   |
| Version discovery service | JM | JM to provide a formal proposal for a light weight version discovery service |   |   |
| Aggregation | IM | Investigate how to achieve aggregation needs |   |   |