GWD-R, GWD-I or GWD-C
NSI-WG
nsi-wg@ogf.org

John MacAuley, ESnet

February 5, 2014

Network Service Interface Discovery Protocol

Status of This Document

Grid Working Document (GWD)

Copyright Notice

Abstract

This document describes the Network Service Agent Interface Discovery Protocol that enables dynamic discovery of protocol metadata for Network Service Agents (NSA) within the Network Service Interface framework. This protocol addresses the key issue of interface version discovery of peer NSA to enable version negotiation; and to determine protocol capabilities supported by that NSA, allowing the bootstrap of peer communications with minimal configuration. A schema is defined describing meta-data associated with an NSA, as well as a RESTful web service to provide an easy to use, searchable, and navigable resource model in support of NSA self-description.

Contents

1 Introduction

Within the NSI reference architecture the Network Services Agent (NSA) is an entity that offers network services. These services can be varied in functionality, and an NSA does not need to offer all services defined within a network. For example, one NSA may offer Connection Services and Topology Services for a specific network, while a second NSA offers Monitoring Services for that same network. In addition, the versions of the services offered can vary from NSA to NSA. The NSI Discovery Service is a metadata service designed to enable self-description of all NSI services and associated protocol interfaces offered by these NSA. Other information relating to the NSA itself, such as software version, administrative contacts, location, peering, and managed networks is also defined as part of the meta-data profile.

This type of dynamic meta-data discovery mechanism is an important aspect of any large-scale distributed system. By making the NSI protocol and its agents more self-descriptive, new features, protocols, or protocol versions can be added to agents within the network and then be discovered by peer agents through this meta-data service. As new features come on line, agents supporting the capabilities can discover compatible peer agents, and then negotiate use of these new features, while older versions of agents within the network remain unaffected. Similarly, newer versions of agents can still negotiate features and communicate with older agent versions using mutually supported versions of the protocol as described in the discovered meta-data.

The NSI Discovery Service is defined as two logical components: the simple protocol for exchange and distribution of meta-data; and the meta-data documents themselves. By abstracting the protocol used for exchange of the data from the data itself, we provide a more generic protocol meeting the requirements for discovery, but also permitting the exchange of other document types in the future.

This document will define both the base discovery protocol and the NSA meta-data document format.

2 Notational Conventions

The key words ‘MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in RFC 2119 [BRADNER], except that the words do not appear in uppercase.

3 Requirements

The following feature requirements have been captured for the NSI Discovery Service. Some may apply to the base protocol, while others will apply specifically to the NSA meta-data document.

Requirement	Description	Functional Area
1	Must be able to discover interfaces and versions of interfaces supported by a peer NSA.	
2	Must be able to discover capabilities of a specific protocol version supported by a peer NSA.	
3	Must be able to describe new protocols, protocol versions, and features without needing to upgrade the protocol.	
4	Must provide support for protocol version negotiation, allowing peer NSA to negotiate a mutually supported version of the protocol.	
5	Shall allow bootstrap of peer communications with minimal configuration.	
6	Must provide equivalent levels of security as existing NSI	

	protocols.	
7	Must support the discovery of multiple independent meta-data document types.	
8	Must support the discovery of multiple versions of the same meta-data document type.	
9	Must be able to detect when new metadata or new versions of existing metadata are available.	
10	Must be able to be notified when new metadata or new versions of existing metadata are available.	
11	Must be able to discover the unique NSA identifier of a peer NSA. Will reduce bootstrap provisioning requirements.	
12	Must be able to discover the NSA software type and version running on a peer NSA. This will allow an NSA to adapt behaviors to specific version of NSA when required.	
13	Must be able to discover the time at which the peer NSA last started to provide uninterrupted service. This is effectively the last restart time of the NSA. A peer discovering a change in this value can initiate recovery procedures.	
14	Must be able to discover administrative contacts associated with the peer NSA.	
15	Must be able to discover the physical location of the peer NSA entity. This can be the location of the server hosting the NSA, or some other location related to the service being offered. This is used for visualization applications and troubleshooting.	
16	Must be able to discover the networks being managed by the peer NSA.	
17	Must be able to discover the compete network control plane topology. This implies discovery of all NSA peering relationships within the network.	
18	Must be able to determine the peer NSA's CS role within the network (Aggregator, uRA, uPA). This will allow an NSA to find a peer aggregator to service CS requests.	
19	Must be able to determine the NSA's CS role of all NSA within the network (Aggregator, uRA, uPA). This is required to compute messaging paths in concert with control plane topology.	
20	Must provide an extensible mechanism to allow additional discovery data to be added to an existing NSA's metadata without needing to upgrade the schema.	

4 NSI Discovery Protocol

5 NSA Discovery Document

The NSA Discovery document encapsulates descriptive meta-data associated with an NSA. The XML schema types used to define the document format are declared in a separate namespace from the core protocol specification, allowing new versions of the NSA discovery schema to be introduced without impacting the base discovery protocol itself. Figure 1 below shows the structure of the NSA discovery document, while Appendix A: NSA discovery document schema contains the full XML schema definition.

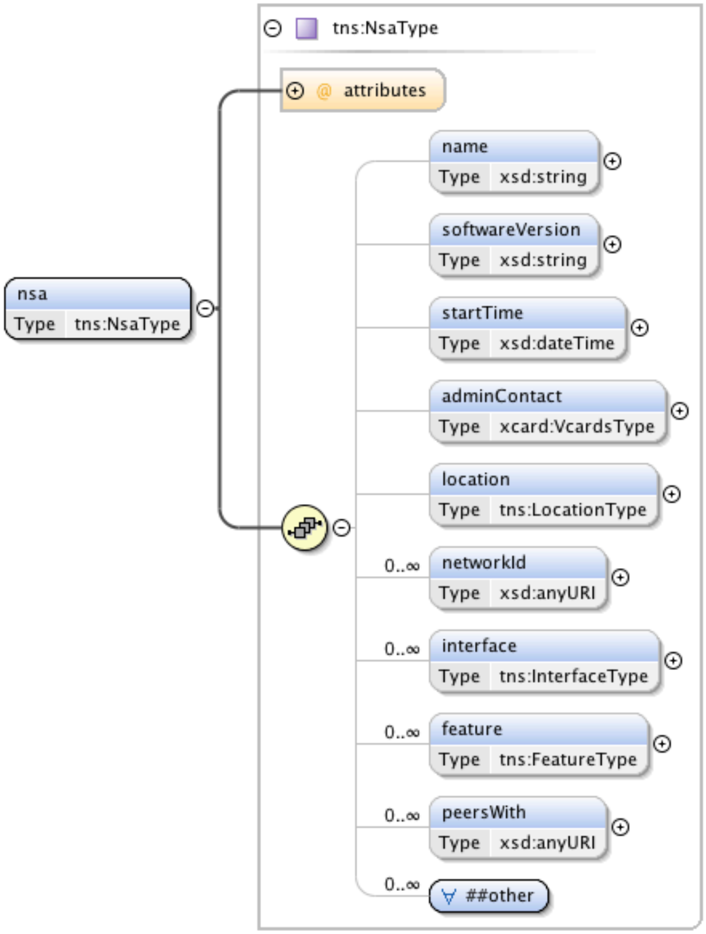

Figure 1 – The NSA discovery document.

The following XML is an example NSA discovery document for a fictitious NSA with globally unique identifier “*urn:ogf:network:example.com:2013:nsa:vixen*”.

```
<tns:nsa xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xcard="urn:ietf:params:xml:ns:vcard-4.0"
         xmlns:tns="http://schemas.ogf.org/nsi/2014/02/discovery/nsa"
    id="urn:ogf:network:example.com:2013:nsa:vixen"
    version="2014-01-04T18:13:51.0Z">
    <name>Example NSA</name>
    <softwareVersion>ExampleNsa-Version-1.0</softwareVersion>
    <startTime>2014-01-01T18:13:51.0Z</startTime>
    <adminContact>
        <xcard:vcard>
            <xcard:uid>
                <xcard:uri>http://www.example.com/santa.claus/santa.asc</xcard:uri>
            </xcard:uid>
            <xcard:prodid><xcard:text>OGF Example Maker // EN</xcard:text></xcard:prodid>
            <xcard:rev><xcard:timestamp>20080424T195243Z</xcard:timestamp></xcard:rev>
            <xcard:kind><xcard:text>individual</xcard:text></xcard:kind>
            <xcard:fn><xcard:text>Saint Nicholas</xcard:text></xcard:fn>
            <xcard:n>
                <xcard:surname>Claus</xcard:surname>
                <xcard:given>Santa</xcard:given>
                <xcard:suffix>Saint</xcard:suffix>
            </xcard:n>
            <xcard:tel><xcard:text>+1 555-555-5555</xcard:text></xcard:tel>
            <xcard:email>
                <xcard:text>santa.claus@theworkshop.example.com</xcard:text>
            </xcard:email>
        </xcard:vcard>
    </adminContact>
    <location>
        <name>Santa's Workshop, The North Pole</name>
        <lat>90.0000</lat>
        <long>0.0000</long>
    </location>
    <networkId>urn:ogf:network:example.com:2013:network:theworkshop</networkId>
    <networkId>urn:ogf:network:example.com:2013:network:candycaneforest</networkId>
    <interface>
        <type>application/vnd.ogf.nsi.discovery.v1+xml</type>
        <href>https://nsa.example.com/discovery</href>
        <describedBy>https://nsa.example.com/discovery/wadl</describedBy>
    </interface>
    <interface>
        <type>application/vnd.ogf.nsi.topology.v1+xml</type>
        <href>https://nsa.example.com/topology.xml</href>
    </interface>
    <interface>
        <type>application/vnd.ogf.nsi.cs.v2.provider+soap</type>
        <href>https://nsa.example.com/connectionProvider</href>
        <describedBy>https://nsa.example.com/connectionProvider/wsdl</describedBy>
    </interface>
    <interface>
        <type>application/vnd.ogf.nsi.cs.v2.requester+soap</type>
        <href>https://nsa.example.com/connectionRequester</href>
        <describedBy>https://nsa.example.com/connectionRequester/wsdl</describedBy>
    </interface>
    <feature type="org.ogf.nsi.cs.v2.role.aggregator"/>
    <feature type="org.ogf.nsi.cs.v2.role.uPA"/>
    <feature type="org.ogf.nsi.cs.v2.commitTimeout">120</feature>
    <peersWith>urn:ogf:network:example.com:2013:nsa:dasher</peersWith>
    <peersWith>urn:ogf:network:example.com:2013:nsa:dancer</peersWith>
    <peersWith>urn:ogf:network:example.com:2013:nsa:prancer</peersWith>
</tns:nsa>
```

The remainder of this section defines the XML types used within the NSA discovery document.

5.1 NsaType

The ***NsaType*** definition models the meta-data elements of an NSA. The id attribute of the NSA must be globally unique as this is the primary identification key used across all NSA for discovery.

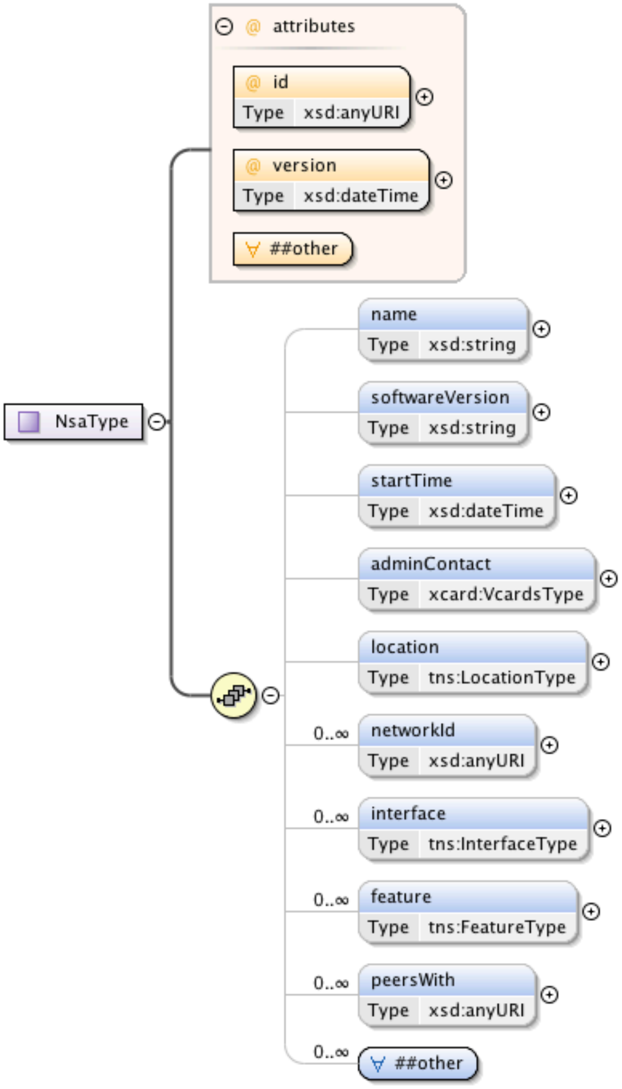

Figure 2 – NsaType.

Parameters

The *nsa* element is defined by the complex type ***NsaType*** that has the following parameters (M = Mandatory, O = Optional):

Parameter	M/O	Description
id	M	The globally unique NSA identifier for this resource.
version	M	The version of this NSA resource based on the date and time the entry was created at the source NSA. This attribute can be used to compare two versions of the document for equality (same version) or to determine the new and older versions through date comparison.
anyAttribute	O	Permit inclusion of attributes from other namespaces for flexible extension without needing to update this schema definition.
name	O	A descriptive name for this NSA resource. This value is typically used for display purposes.
softwareVersion	O	A descriptive string describing the NSA software type and version. This value will allow a peer NSA to adapt behaviors to specific versions of an NSA when required.
startTime	O	The time at which this NSA last started to provide uninterrupted service.

		This is effectively the last restart time of the NSA. A peer discovering a change in this value can initiate recovery procedures.
adminContact	O	A list of zero or more administrative contacts associated with this NSA.
location	O	The physical location of the logical NSA resource. This can be the location of the server hosting the NSA, or some other location related to the service being offered.
networkId	O	A list of zero or more network identifiers for which this NSA is providing the listed service interfaces and features. These network identifiers can be mapped into network topology (the topologyId) to determine the network resources being managed by this NSA.
interface	O	A list of zero or more service interfaces supported by the NSA.
peersWith	O	A list of zero or more NSA identifiers enumerating the peer NSA that have trusted control plane relationships with this NSA.
any element	O	Provides a flexible mechanism allowing additional elements to be provided from other namespaces without needing to update this schema definition.

5.2 VcardsType

The *adminContact* field of the ***NsaType*** definition uses the standard vCard XML Representation [RFC 6351]. The ***VcardsType*** supports a list of *vcards* that can be used to fully model administrator contact information. Due to the size of the structure it will not be reproduced here.

5.3 LocationType

The ***LocationType*** definition models the location elements of an NSA. A Location is a reference to a geographical location or area for the NSA.

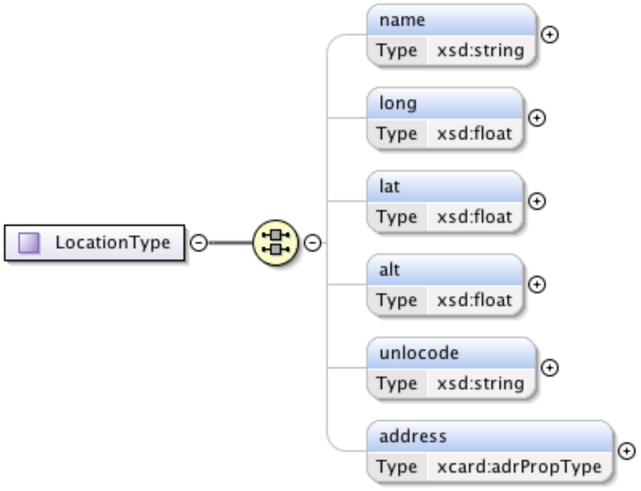

Figure 3 – LocationType.

Parameters

The *location* element is defined by the complex type ***LocationType*** that has the following parameters (M = Mandatory, O = Optional):

Parameter	M/O	Description
name	O	A human readable string naming this location.
long	O	The longitude of the NSA in WGS84 coordinate system (in decimal degrees).
lat	O	The latitude of the NSA in WGS84 coordinate system (in decimal degrees).
alt	O	The altitude of the NSA in WGS84 coordinate system (in decimal meters).
unlocode	O	The UN/LOCODE location identifier for the NSA location.
address	O	The address of the NSA location specified in vCard address format.

5.4 InterfaceType

The ***InterfaceType*** definition models an NSA protocol interface. This type encapsulates the meta-data needed to determine the version, location, and schema associated with a specific NSA interface.

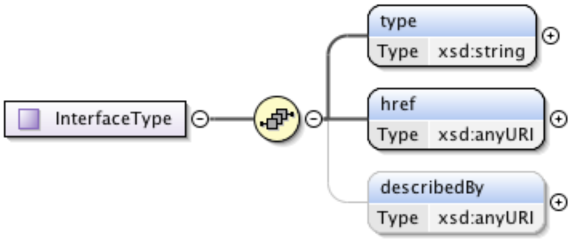

Figure 4 – InterfaceType.

For example, the first *interface* entry below identifies the NSI Discovery Protocol Version 1 XML encoded representation. The *type* element describes the specific version of the discovery interface, as well as the media encoding used on the interface. The *href* element provides the protocol endpoint used to access this interface. The optional *describedBy* element provides a reference to the meta-data document formally describing the interface. In this case, a WADL document is available describing the discovery REST interface.

```
<interface>
    <type>application/vnd.ogf.nsi.discovery.v1+xml</type>
    <href>https://nsa.example.com/discovery</href>
    <describedBy>https://nsa.example.com/discovery/wadl</describedBy>
</interface>
```

This second entry also defines an interface for the NSI Discovery Protocol Version 1, but instead of XML, this is a definition for a JSON representation:

```
<interface>
    <type> application/vnd.ogf.nsi.discovery.v1+json</type>
    <href>https://nsa.example.com/discovery</href>
    <describedBy>https://nsa.example.com/discovery/wadl</describedBy>
</interface>
```

It is also possible to defined an interface that does not contain the describedBy element. This can be used in situations where dynamically discovering the interface description is not required:

```
<interface>
    <type> application/vnd.ogf.nsi.topology.v1+xml</type>
    <href>https://nsa.example.com/topology.xml</href>
</interface>
```

Parameters
The *interface* element is defined by the complex type ***InterfaceType*** that has the following parameters (M = Mandatory, O = Optional):

Parameter	M/O	Description
type	M	The unique string identifying the type and version of the NSA interface. Application Internet media types (Content-types) are used to identify the NSI interface, version, and supported

		encoding type.
href	M	Contains the protocol endpoint for the interface identified in this interface reference.
describedBy	O	This attribute contains a reference to the WSDL or WADL file corresponding to this interface's version (if available).

5.5 FeatureType

The **FeatureType** definition is a simple type value pair used to model an NSA feature within the network. This type is left underspecified so that external values can be defined as additional features as protocol interfaces are introduced.

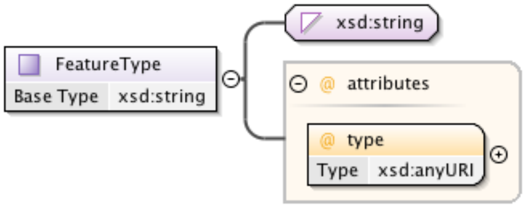

Figure 5 - FeatureType

As an example we can model the NSA's CS "role" within the network as shown below:

```
<feature type="org.ogf.nsi.cs.v2.role.aggregator"/>
<feature type="org.ogf.nsi.cs.v2.role.uPA"/>
<feature type="org.ogf.nsi.cs.v2.role.uRA"/>
```

Notice that in the previous example there is no value associated with the feature type. To illustrate a type/value combination, we could model the NSI CS 2.0 reservation commit timeout value for an NSA as follows:

```
<feature type="org.ogf.nsi.cs.v2.commitTimeout">120</feature>
```

Parameters
The *feature* element is defined by the simple type ***FeatureType*** that has the following parameters (M = Mandatory, O = Optional):

Parameter	M/O	Description
type	M	Identifies the type of role modeled by the supplied value.
value	M	The optional string value associated with the type.

6 Security Considerations

Please refer to RFC 3552 [RESCORLA] for guidance on writing a security considerations section. This section is required in all documents, and should not just say “there are no security considerations.” Quoting from the RFC:

> “Most people speak of security as if it were a single monolithic property of a protocol or system, however, upon reflection, one realizes that it is clearly not true. Rather, security is a series of related but somewhat independent properties. Not all of these properties are required for every application.

> We can loosely divide security goals into those related to protecting communications (COMMUNICATION SECURITY, also known as COMSEC) and those relating to protecting systems (ADMINISTRATIVE SECURITY or SYSTEM SECURITY). Since communications are carried out by systems and access to systems is through communications channels, these goals obviously interlock, but they can also be independently provided."

7 Glossary

Recommended but not required.

8 Contributors

John H. MacAuley, ESnet, macauley@es.net

9 Intellectual Property Statement

The OGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights, which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

10 Disclaimer

This document and the information contained herein is provided on an "As Is" basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

11 Full Copyright Notice

The limited permissions granted above are perpetual and will not be revoked by the OGF or its successors or assignees.

12 Appendix A: NSA discovery document schema

The following XSD is captured from the *ogf_nsi_discovery_nsa_v1_0.xsd* schema file that is the official source for the NSA discovery document schema.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
The OGF takes no position regarding the validity or scope of any intellectual
property or other rights that might be claimed to pertain to the implementation
or use of the technology described in this document or the extent to which any
license under such rights might or might not be available; neither does it
represent that it has made any effort to identify any such rights.  Copies of
claims of rights made available for publication and any assurances of licenses
to be made available, or the result of an attempt made to obtain a general
license or permission for the use of such proprietary rights by implementers or
users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights,
patents or patent applications, or other proprietary rights which may cover
technology that may be required to practice this recommendation.  Please
address the information to the OGF Executive Director.

This document and the information contained herein is provided on an "As Is"
basis and the OGF disclaims all warranties, express or implied, including but
not limited to any warranty that the use of the information herein will not
infringe any rights or any implied warranties of merchantability or fitness
for a particular purpose.

Copyright (C) Open Grid Forum (2009-2012). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and
derivative works that comment on or otherwise explain it or assist in its
implementation may be prepared, copied, published and distributed, in whole or
in part, without restriction of any kind, provided that the above copyright
notice and this paragraph are included on all such copies and derivative works.
However, this document itself may not be modified in any way, such as by removing
the copyright notice or references to the OGF or other organizations, except as
needed for the purpose of developing Grid Recommendations in which case the
procedures for copyrights defined in the OGF Document process must be followed,
or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by
the OGF or its successors or assignees.

Open Grid Forum NSI Discovery Types (NSA) v1.0.

Description: This is the NSA document type schema defined for use in the OGF NSI
Discovery Protocol v1.0. Comments and questions can be directed to the mailing
list group mailing list (nsi-wg@ogf.org).
-->
<xsd:schema targetNamespace="http://schemas.ogf.org/nsi/2014/02/discovery/nsa"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xcard="urn:ietf:params:xml:ns:vcard-4.0"
    xmlns:tns="http://schemas.ogf.org/nsi/2014/02/discovery/nsa">

    <xsd:annotation>
        <xsd:documentation xml:lang="en">
            This is an XML schema document describing the NSA element of the
            OGF NSI Interface Discovery Protocol v1.0.  There is a corresponding
            document providing a description of the RESTful service definition
            and protocol specific types.

            Within the NSI reference architecture the Network Services Agent
            (NSA) is an entity that offers network services.  These services
            can be varied in functionality, and an NSA does not need to offer
            all services defined within a network.  For example, one NSA may
            offer Connection Services and Topology Services for a specific
            network, while a second NSA offers Monitoring Services for that
            same network.  In addition, the versions of the services offered
            can vary from NSA to NSA.  The NSI Discovery Protocol is a metadata
            service designed to enable self-description of all NSI services
            and associated protocol interfaces offered by these NSA.

            The NSI Discovery schema allows an NSA to describe the
            interfaces and versions of interfaces that it supports.  Through
            the REST API access methods defined, an NSA can dynamically
            discover interfaces and capabilities supported by a peer NSA,
            perform protocol version negotiation based on the supplied
            metadata, identify protocol endpoints, and bootstrap peer
            communications with minimal configuration.

            This document encapsulates the types used to model meta-data
            associated with an NSA.  By defining these type in a separate
            namespace, it is hoped that new versions of the meta-data will not
            impact the base discovery protocol.
        </xsd:documentation>
    </xsd:annotation>

    <!-- Import additional standard name spaces. -->
    <xsd:import namespace="urn:ietf:params:xml:ns:vcard-4.0" schemaLocation="xCard.xsd"/>

    <!-- ******************************************************************
         *                      XML element types                         *
         ****************************************************************** -->

    <!-- NSA resource definition. -->
    <xsd:element name="nsa" type="tns:NsaType" />

    <!-- ******************************************************************
         *                        XML base types                          *
         ****************************************************************** -->

    <xsd:complexType name="NsaType">
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                This is the type definition for meta-data associated with an
                NSA resource.

                Attributes:

                id - The globally unique NSA identifier for this resource.

                version - The version of this NSA resource based on the date
                and time the entry was created at the source NSA.  This
                attribute can be used to compare two versions of the document
                for equality (same version) or to determine the new and older
                versions through date comparison.

                anyAttribute - Permit inclusion of attributes from other namespaces
                for flexible extension without needing to update this schema
                definition.

                Elements:

                name - A descriptive name for this NSA resource.  This value is
                typically used for display purposes.

                softwareVersion - A descriptive string describing the NSA software
                type and version.   This value will allow a peer NSA to adapt
                behaviors to specific versions of an NSA when required.

                startTime - The time at which this NSA last started to provide
                uninterrupted service.   This is effectively the last restart
                time of the NSA.  A peer discovering a change in this value
                can initiate recovery procedures.

                adminContact - A list of zero or more administrative contacts
                associated with this NSA.

                location - The physical location of the logical NSA resource.
                This can be the location of the server hosting the NSA, or
                some other location related to the service being offered.

                networkId - A list of zero or more network identifiers for which
                this NSA is providing the listed service interfaces and
                features.  These network identifiers can be mapped into network
                topology to determine the network resources being managed by
                this NSA.

                interface - A list of zero or more service interfaces supported
                by the NSA.

                peersWith - A list of zero or more NSA identifiers enumerating
                the peer NSA that have set up a trusted control plane relationship
                with this NSA.

                any - Provides a flexible mechanism allowing additional elements
                to be provided from other namespaces without needing to update
                this schema definition.
            </xsd:documentation>
        </xsd:annotation>
            <xsd:sequence>
                <xsd:element name="name" type="xsd:string" minOccurs="0" />
                <xsd:element name="softwareVersion" type="xsd:string" minOccurs="0" />
                <xsd:element name="startTime" type="xsd:dateTime" minOccurs="0" />
                <xsd:element name="adminContact" type="xcard:VcardsType" minOccurs="0" />
                <xsd:element name="location" type="tns:LocationType" minOccurs="0" />
                <xsd:element name="networkId" type="xsd:anyURI" minOccurs="0"
                      maxOccurs="unbounded" />
                <xsd:element name="interface" type="tns:InterfaceType" minOccurs="0"
                      maxOccurs="unbounded" />
                <xsd:element name="feature" type="tns:FeatureType" minOccurs="0"
                      maxOccurs="unbounded" />
                <xsd:element name="peersWith" type="xsd:anyURI" minOccurs="0"
                      maxOccurs="unbounded" />
                <xsd:any namespace="##other" processContents="lax" minOccurs="0"
                      maxOccurs="unbounded"/>
            </xsd:sequence>
            <xsd:attribute   name="id"      use="required" type="xsd:anyURI" />
            <xsd:attribute   name="version" use="required" type="xsd:dateTime" />
            <xsd:anyAttribute namespace="##other" processContents="lax" />
    </xsd:complexType>

    <xsd:complexType name="LocationType">
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                This is a type definition modeling the location of an NSA.  A
                Location is a reference to a geographical location or area for
                the NSA.

                Elements:

                name  - A human readable string naming this location.

                long - The longitude of the NSA in WGS84 coordinate system (in
                decimal degrees).

                lat - The latitude of the NSA in WGS84 coordinate system (in
                decimal degrees).

                alt  - The altitude of the NSA in WGS84 coordinate system (in
                decimal meters).
                unlocode - The UN/LOCODE location identifier for the NSA
                location.

                address - The address of the NSA location specified using the
                vCard address format.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:all>
            <xsd:element name="name"     type="xsd:string"        minOccurs="0" />
            <xsd:element name="long"     type="xsd:float"         minOccurs="0" />
            <xsd:element name="lat"      type="xsd:float"         minOccurs="0" />
            <xsd:element name="alt"      type="xsd:float"         minOccurs="0" />
            <xsd:element name="unlocode" type="xsd:string"        minOccurs="0" />
            <xsd:element name="address"  type="xcard:adrPropType" minOccurs="0" />
        </xsd:all>
    </xsd:complexType>

    <xsd:complexType name="InterfaceType">
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                Type definition that models an NSA protocol interface.  This
                type encapsulates the meta-data needed to determine the version,
                location, and schema associated with a specific NSA interface.

                Elements:

                type - The unique string identifying the type and version of
                the NSA interface.  Application Internet media types
                (Content-types)  are used to identify the NSI interface,
                version, and supported encoding type.  For example, the
                first string below identifies the NSI Interface Discovery
                Protocol Version 1 XML encoded representation, while the
                second string identifies the same protocol and version, but
                the JSON representation:

                type="application/vnd.ogf.nsi.discovery.v1+xml"
                type="application/vnd.ogf.nsi.discovery.v1+json"

                href - This attribute contains the protocol endpoint for the
                interface identified in this interface reference.  For example, the
                following URL provides the protocol endpoint for the interface type
                identified in this interface reference.

                href="https://nsa.ogf.org/discovery"

                describedBy - This attribute contains a reference to the WSDL
                or WADL file corresponding to this interface's version (if
                available).  For example, the following URL provides the
                location for a WADL description of the NSI Interface Discovery
                Protocol Version 1.

                describedBy="https://nsa.ogf.org/discovery/wadl"
            </xsd:documentation>
        </xsd:annotation>
        <xsd:sequence>
            <xsd:element name="type"        type="xsd:string" />
            <xsd:element name="href"        type="xsd:anyURI" />
            <xsd:element name="describedBy" type="xsd:anyURI" minOccurs="0" />
        </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="FeatureType">
        <xsd:annotation>
            <xsd:documentation xml:lang="en">
                Type definition for an NSA feature within the network.  This type
                is left underspecified so that external values can be defined
                as additional features and protocol interfaces are introduced.
                As an example we can model the NSA's CS "role" within the network
                as shown below:

                <feature type="org.ogf.nsi.cs.v2.role.aggregator"/>
                <feature type="org.ogf.nsi.cs.v2.role.uPA"/>
                <feature type="org.ogf.nsi.cs.v2.role.uRA"/>

                We could also model the NSI CS 2.0 reservation commit timeout
                value for an NSA:

                <feature type="org.ogf.nsi.cs.v2.commitTimeout">120</feature>

                Attributes:

                type - Identifies the type of role modeled by the supplied
                value.

                value - The optional string value associated with the type.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:simpleContent>
            <xsd:extension  base="xsd:string">
                <xsd:attribute  name="type"  type="xsd:anyURI"  use="required"/>
            </xsd:extension>
        </xsd:simpleContent>
    </xsd:complexType>
</xsd:schema>
```

References

[BRADNER] Scott Bradner. Key Words for Use in RFCs to Indicate Requirement Levels, RFC 2119. The Internet Society. March 1997. http://tools.ietf.org/html/rfc2026

[RFC 6350] Simon Perreault. vCard Format Specification RFC 6350 (Standards Track), August 2011. URL http://tools.ietf.org/html/rfc6350.

[RFC 6351] S. Perreault. xCard: vCard XML Representation RFC 6351 (Standards Track), August 2011. URL http://tools.ietf.org/html/rfc6351.