Using NVDL with XML Signatures

Rob Miller
What is NVDL?

• NVDL = Namespace-based Validation Dispatching Language
• NVDL is an XML technology
• NVDL is an ISO standard
• NVDL enables you to independently develop data, then assemble the data into a single document, and then validate that compound document
Example
Scenario:
You've created an XML Schema to track moving targets
Moving Target Schema
Moving Target Instance \textit{conforms to} Moving Target Schema
Later, you decide that you want to embed* an XML signature into the instances

* Enveloped XML Signature
XML Signature Schema

conforms to

Moving Target Instance

<Signature>
  ...
</Signature>

xmlDSig-Core-Schema.xsd
If the author of the Moving Target Schema didn't anticipate the use of XML Signatures ...
Moving Target Schema

XML Schema Validator

Error!
A solution?
Modify the Moving Target Schema to import the XML Signature schema

XML Signature Schema

Moving Target Schema

import
Two problems with this solution
Tightly coupled schemas: you have to modify Moving Target Schema to import the XML Signature Schema and you have to insert an element declaration that references an element or type within the XML Signature schema. If at a later date you no longer want to use XML Signature, or you want it nested at a different location within your documents, then you will have to remove/alter your schema.
**Doesn't scale**: after XML Signature you may need to add Dublin Core (metadata), security markings, encryption, and so forth. You will find yourself in constant XML Schema update mode. ($$$)
A nice solution →
XML Signature Schema

conforms to

Moving Target Instance

<Signature>
  ...
</Signature>

conforms to

Moving Target Schema
XML Signature Schema

Moving Target Instance

<Signature>
  ...
</Signature>

XML Schema Validator

Okay!

Moving Target Schema

XML Schema Validator

Okay!
Moving Target Instance

<Signature>
...
</Signature>

Compound document
Schema validator: please validate the XML Signature portion against `xmlDSig-core-schema.xsd` and the rest against `moving-target.xsd`
Schema validator: please validate the XML Signature portion against xmldsig-core-schema.xsd and the rest against moving-target.xsd

<Signature>
...
</Signature>
English prose isn't very good for machines. Want to express this in a way that is good for machines.

Schema validator: please validate the XML Signature portion against xmldsig-core-schema.xsd and the rest against moving-target.xsd

Moving Target Instance

<Signature>
...
</Signature>
XML!
XML

Moving Target Instance

<Signature>
...
</Signature>

Need a standardized XML vocabulary
NVDL is a standardized XML vocabulary for expressing how the instance document should be "sectioned" and how each section should be validated.

Moving Target Instance

<NSignature>
...
</NSignature>
A Few Details
Schema-Neutral Assembly of Data Components

DTD
Schematron
Relax NG
XML Schema
Schema-Neutral Assembly of Data Components

<Moving-Target>
  <Target-ID>Charlie 1</Target-ID>
  <Location>
    <Latitude>129.32</Latitude>
    <Longitude>90.91</Longitude>
  </Location>
  ...
  <Signature>
    <SignedInfo>
      <CanonicalizationMethod
          Algorithm="http://...c14n-20010315"/>
      <SignatureMethod
          Algorithm="http://...xmldsig#dsa-sha1"/>
      ...
    </SignedInfo>
  </Signature>
</Moving-Target>
The Whole Document Conforms to ???

Each individual data component conforms to a schema, but what does the whole document conform to?

```xml
<Moving-Target>
  <Target-ID>Charlie 1</Target-ID>
  <Location>
    <Latitude>129.32</Latitude>
    <Longitude>90.91</Longitude>
  </Location>
  ...
  <Signature>
    <SignedInfo>
      <CanonicalizationMethod
        Algorithm="http://...c14n-20010315"/>
      <SignatureMethod
        Algorithm="http://...xmldsig#dsa-shal"/>
      ...
    </SignedInfo>
  </Signature>
</Moving-Target>
```
Meta-Schema

• What is needed is a meta-schema.
• A meta-schema specifies the schemas that may be collectively used to create an XML instance document. Thus, a meta-schema is a schema for schemas.
NVDL is a Meta-Schema Language

• With NVDL you can make statements like this:

  The XML instance document must be comprised of an Moving Target Data Component and an XML Signature Data Components.
Data Components are Identified by their Namespace

These namespace declarations enable an NVDL processor to partition (section) this XML instance document.
NVDL Processor "Sections" the XML Instance Document

```
<Moving-Target xmlns="http://www.dod.gov/moving-target#">
  <Target-ID>Charlie 1</Target-ID>
  <Location>
    <Latitude>129.32</Latitude>
    <Longitude>90.91</Longitude>
  </Location>
  ...
</Moving-Target>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://...c14n-20010315"/>
    <SignatureMethod
      Algorithm="http://...xmlsig#dsa-sha1"/>
    ...
  </SignedInfo>
</Signature>
```

```
<Moving-Target xmlns="http://www.dod.gov/moving-target#">
  <Target-ID>Charlie 1</Target-ID>
  <Location>
    <Latitude>129.32</Latitude>
    <Longitude>90.91</Longitude>
  </Location>
  ...
</Moving-Target>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://...c14n-20010315"/>
    <SignatureMethod
      Algorithm="http://...xmlsig#dsa-sha1"/>
    ...
  </SignedInfo>
</Signature>
```
... and then Validates each Section

<Moving-Target xmlns="http://www.dod.gov/moving-target#">
  <Target-ID>Charlie 1</Target-ID>
  <Location>
    <Latitude>129.32</Latitude>
    <Longitude>90.91</Longitude>
  </Location>
  ...
</Moving-Target>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://...c14n-20010315"/>
    <SignatureMethod
      Algorithm="http://...xmldsig#dsa-sha1"/>
    ...
  </SignedInfo>
</Signature>

<Signature xmlns="http://www.dod.gov/moving-target#">
  <Target-ID>Charlie 1</Target-ID>
  <Location>
    <Latitude>129.32</Latitude>
    <Longitude>90.91</Longitude>
  </Location>
  ...
</Moving-Target>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://...c14n-20010315"/>
    <SignatureMethod
      Algorithm="http://...xmldsig#dsa-sha1"/>
    ...
  </SignedInfo>
</Signature>
"Dispatch"

- The terminology is, "The NVDL processor dispatches each data component to the appropriate schema validator."
The **NVDL Meta-Schema**
Instructs the NVDL Processor

```
<Moving-Target xmlns="http://www.dod.gov/moving-target#">
   <Target-ID>Charlie 1</Target-ID>
   <Location>
      <Latitude>129.32</Latitude>
      <Longitude>90.91</Longitude>
   </Location>
   ...
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod
            Algorithm="http://...c14n-20010315"/>
         <SignatureMethod
            Algorithm="http://...xmldsig#dsa-sha1"/>
         ...
      </SignedInfo>
   </Signature>
</Moving-Target>
```
The NVDL Meta-Schema Instructs the NVDL Processor

"The XML instance document must be comprised of a Moving Target Data Component and an XML Signature Data Component. The Moving Target component must be validated against Moving-Target.rng. The XML Signature component must be validated against xmldsig-core-schema.xsd."
Wrap-up
The folks at Oxygen XML have created a Java implementation of an NVDL processor, called oNVDL. It can be downloaded from:

- Download the zip file and then unzip it. To use it, at a command line type this:

  ```
  java -jar path-to-the-oxygen-onvdl-folder/onvdl/bin/onvdl.jar name-of-nvdl-file.nvdl name-of-xml-file.xml
  ```

SnRNV (Small nano Reconstruction NVDL Validator). SnRNV is a streaming NVDL validator, dispatcher, and reconstructor, which can be used with other JAXP based XML validators such as Xerces, MSV, and Jing (Note that you need JARV-JAXP bridge to use MSV or Jing). SnRNV can be downloaded from:

- [http://www.asahi-net.or.jp/~eb2m-mrt/nvdl/SnRNV-1.0.zip](http://www.asahi-net.or.jp/~eb2m-mrt/nvdl/SnRNV-1.0.zip)

jNVDL is also a Java-based implementation of an NVDL processor. It can be downloaded from:

- [http://jnvdl.sourceforge.net/about-jnvdl.html](http://jnvdl.sourceforge.net/about-jnvdl.html)
Who's Using NVDL

- OOXML
- Ecma-376 Office Open XML
- W3C Internationalization Tag Set
- W3C SVG Tiny 1.2
- Docbook v5.0
NVDL Tutorial

http://www.xfront.com/nvdl/