SCAP 1.2 Data Models

Adam Halbardier
Booz Allen Hamilton
Supporting NIST

To pass the time while you wait:

A person has 10 trees and plants them in 5 rows of 4 trees each. What configuration makes that possible?

Agenda

- SCAP Source Data Stream
- SCAP Result Data Stream
- Signing SCAP Source Data Stream
- Signing SCAP Result Data Stream

Agenda

- SCAP Source Data Stream
- SCAP Result Data Stream
- Signing SCAP Source Data Stream
- Signing SCAP Result Data Stream

History of SCAP Source Format

- SCAP 1.0 and 1.1 specify file naming convention for SCAP components
  - xxxxxccdf.xml
  - xxxxoval.xml
  - xxxxpatches.xml
  - xxxxcpe-dictionary.xml
  - xxxxcpe-oval.xml
- SP 800-126 does not specify the package format for the components
  - ZIP?
  - CAB?
  - Directory?

Deficiency of Existing Source Format

- Lack of package specificity
- File-based -> limits stream-based implementations
- Ties SCAP logical level concerns (file names) to low-level specification data (see example on next page)

Example: Logical Level Blended

- ZIP Package
  - sample-xccdf.xml

```
<xccdf:check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <xccdf:check-content-ref href="sample-oval.xml" name="oval:gov.nist:def:1"/>
</xccdf:check>
```

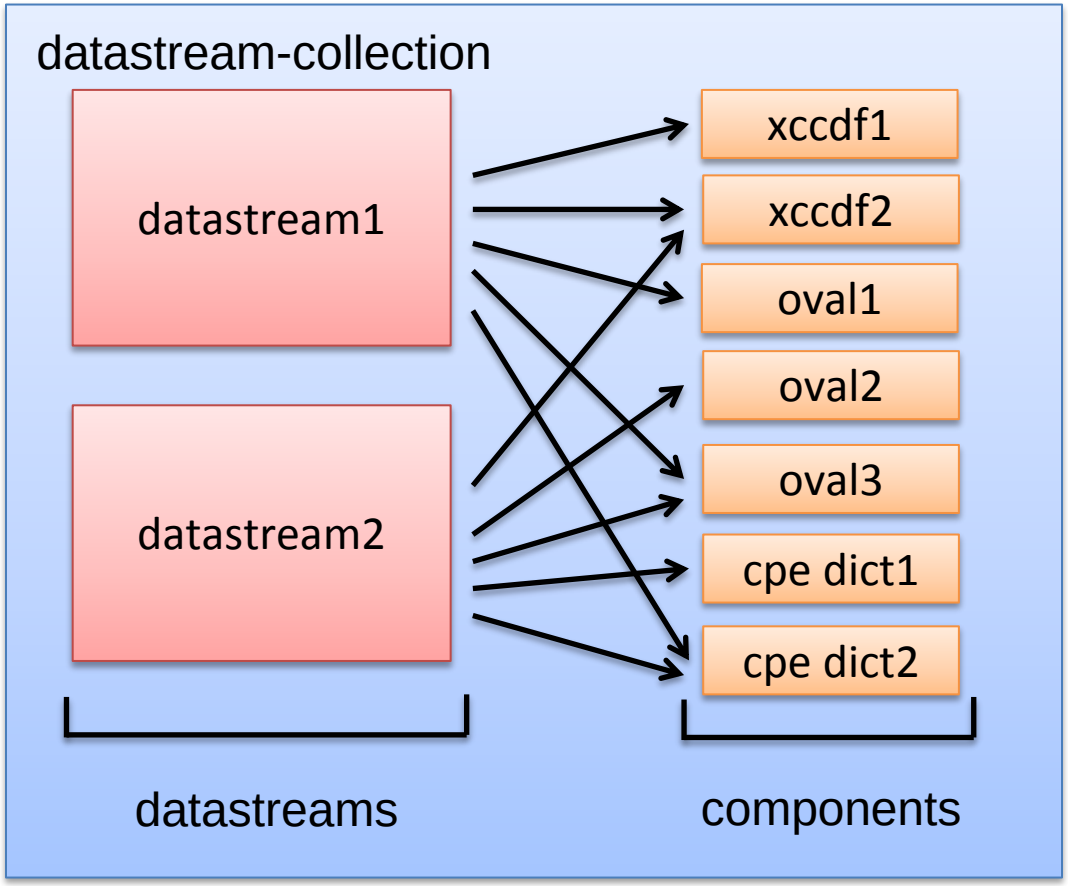
  - sample-oval.xml

```
<oval-def:definition class="compliance" id="oval:gov.nist:def:1" version="1">
  ...
</oval-def:definition>
```

Solution?

An SCAP source data stream that is XML based and provides logical abstractions of the references

Approach


datastream-collection
datastream1
datastream2
xccdf1
xccdf2
oval1
oval2
oval3
cpe dict1
cpe dict2
datastreams
components

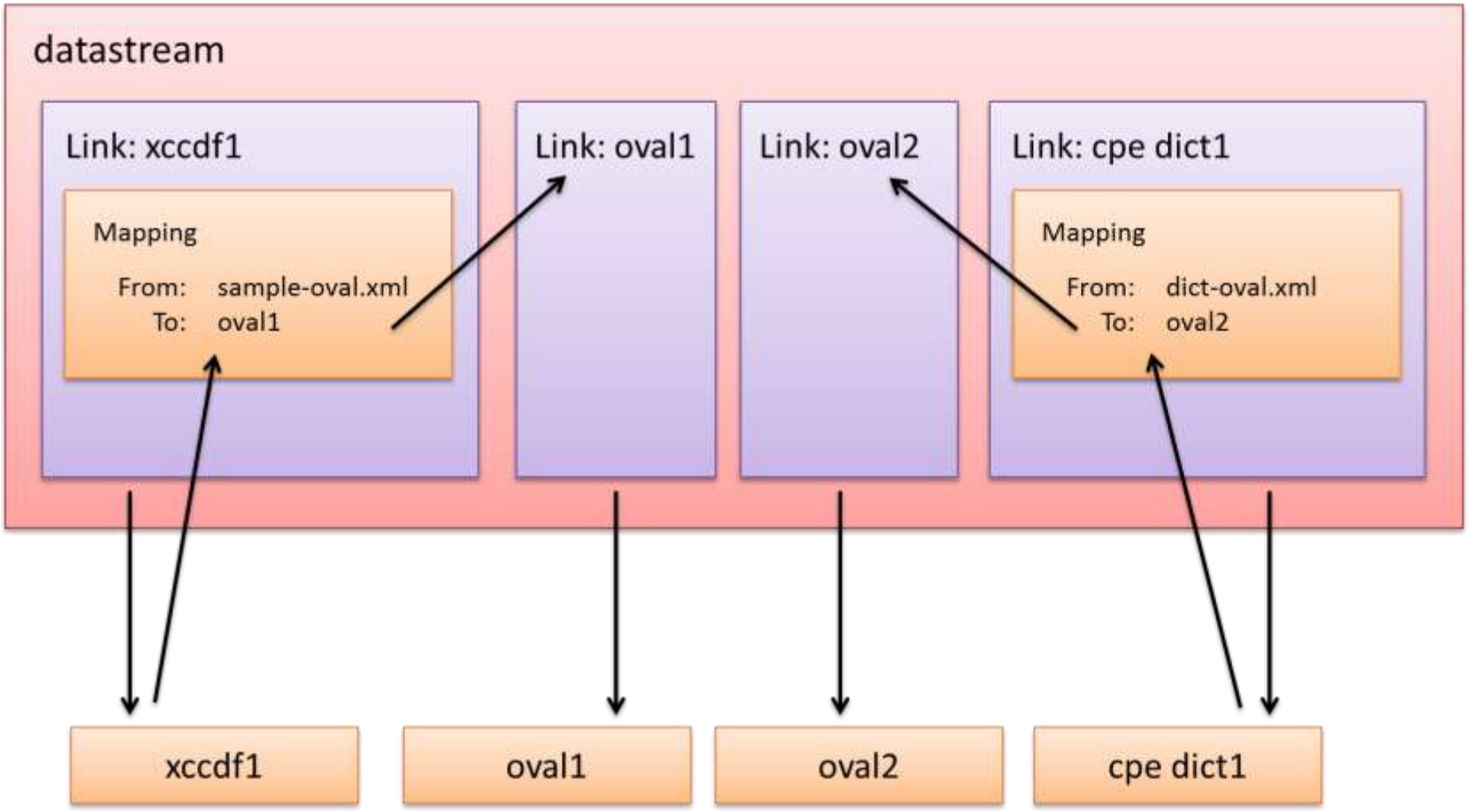
Advantages

- Multiple SCAP source data streams can be represented in a single package.
- Components are easily reusable across data streams.
- Components and data streams can be added and removed from the collection in a modular fashion.
- A well-defined format for the SCAP source content eliminates ambiguity of the physical representation of the content.
- A single XML file approach enables content validation options such as XML schema and Schematron validation.
- It offers the ability to handle any arbitrary number of checklist, check, and dictionary components.

Advantages (cont.)

- It allows use of multiple OVAL versions simultaneously.
- A single XML file approach reduces complexity in creating, validating and managing XML Digital Signatures.
- It reduces the complexity of using SCAP data streams in service implementations (e.g., SOAP Web Services, REST).
- In an environment using dynamic tasking commands, SCAP content can be built on-the-fly based on the needs of a task.

Datastream Details



Advantages

- The dereferencing of component links is mapped at the SCAP logical level, allowing components to be easily reused without modifying the content
- Digital signatures can be kept intact for components

```
<data-stream-collection id="scap_gov.nist_collection_minimal.zip">
 <data-stream id="scap_gov.nist_datastream_minimal.zip" scap-version="1.2" timestamp="2011-09-26T04:36:47"
  use-case="CONFIGURATION">
  <dictionaries>
   <component-ref id="scap_gov.nist_cref_minimal-cpe-dictionary.xml"
    xlink:href="#scap_gov.nist_comp_minimal-cpe-dictionary.xml">
    <cat:catalog>
     <cat:uri name="minimal-cpe-oval.xml" uri="#scap_gov.nist_cref_minimal-cpe-oval.xml"/>
    </cat:catalog>
   </component-ref>
  </dictionaries>
  <checklists>
   <component-ref id="scap_gov.nist_cref_minimal-xccdf.xml" xlink:href="#scap_gov.nist_comp_minimal-xccdf.xml">
    <cat:catalog>
     <cat:uri name="minimal-oval.xml" uri="#scap_gov.nist_cref_minimal-oval.xml"/>
    </cat:catalog>
   </component-ref>
  </checklists>
  <checks>
   <component-ref id="scap_gov.nist_cref_minimal-oval.xml" xlink:href="#scap_gov.nist_comp_minimal-oval.xml"/>
   <component-ref id="scap_gov.nist_cref_minimal-cpe-oval.xml" xlink:href="#scap_gov.nist_comp_minimal-cpe-
oval.xml"
    />
  </checks>
 </data-stream>
```

```
<component id="scap_gov.nist_comp_minimal-xccdf.xml" timestamp="2011-09-26T04:36:47">
  <xccdf:Benchmark id="xccdf_gov.nist_benchmark_minimal-xccdf"
   style="SCAP_1.2" xml:lang="en-US">
   <xccdf:Rule id="xccdf_gov.nist_rule_test_rule1" selected="true" weight="10.0">
    <xccdf:check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
     <xccdf:check-content-ref href="minimal-oval.xml" name="oval:gov.nist.test.compliance:def:1"/>
    </xccdf:check>
   </xccdf:Rule>
  </xccdf:Benchmark>
 </component>
 <component id="scap_gov.nist_comp_minimal-oval.xml" timestamp="2011-09-26T04:36:47">
  <oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5">
   <definition class="compliance" id="oval:gov.nist.test.compliance:def:1" version="1">
   </definition>
  </oval_definitions>
 </component>
 <component id="scap_gov.nist_comp_minimal-cpe-oval.xml" timestamp="2011-09-26T04:36:47">
 </component>
 <component id="scap_gov.nist_comp_minimal-cpe-dictionary.xml" timestamp="2011-09-26T04:36:47">
  <cpe-list xmlns="http://cpe.mitre.org/dictionary/2.0">
   <cpe-item name="cpe:/o:microsoft:windows_vista">
    <check href="minimal-cpe-oval.xml" system="http://oval.mitre.org/XMLSchema/oval-definitions-
5">oval:gov.nist.test.inventory:def:1</check>
   </cpe-item>
  </cpe-list>
 </component>
</data-stream-collection>
```

Agenda

- SCAP Source Data Stream
- SCAP Result Data Stream
- Signing SCAP Source Data Stream
- Signing SCAP Result Data Stream

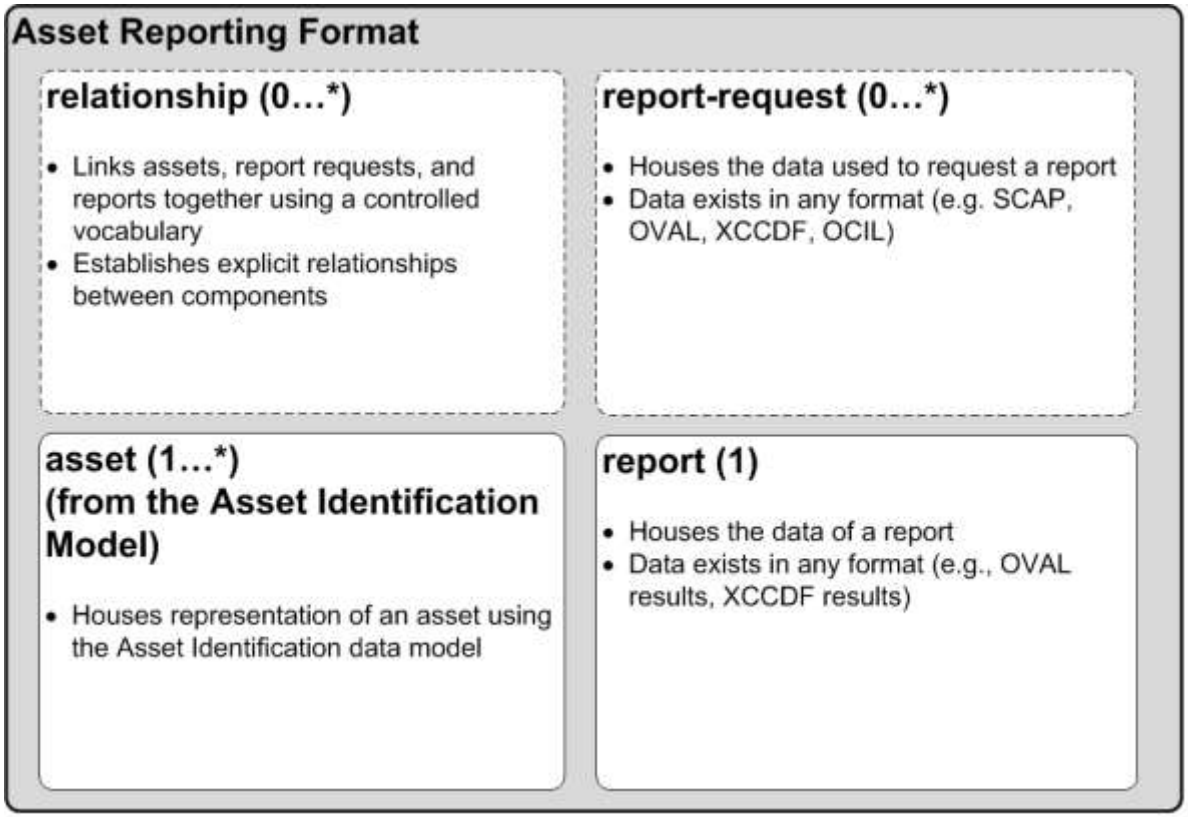
History of SCAP Result Format

- SCAP 1.1 specify file naming convention for SCAP components results
  - xxxxxccdf-res.xml
  - xxxxoval-res.xml
  - xxxxpatches-res.xml
  - xxxxcpe-dictionary-res.xml
  - xxxxcpe-oval-res.xml
- SP 800-126 does not specify the package format for the results
  - ZIP?
  - Directory?
  - Other?

Why develop a results format?

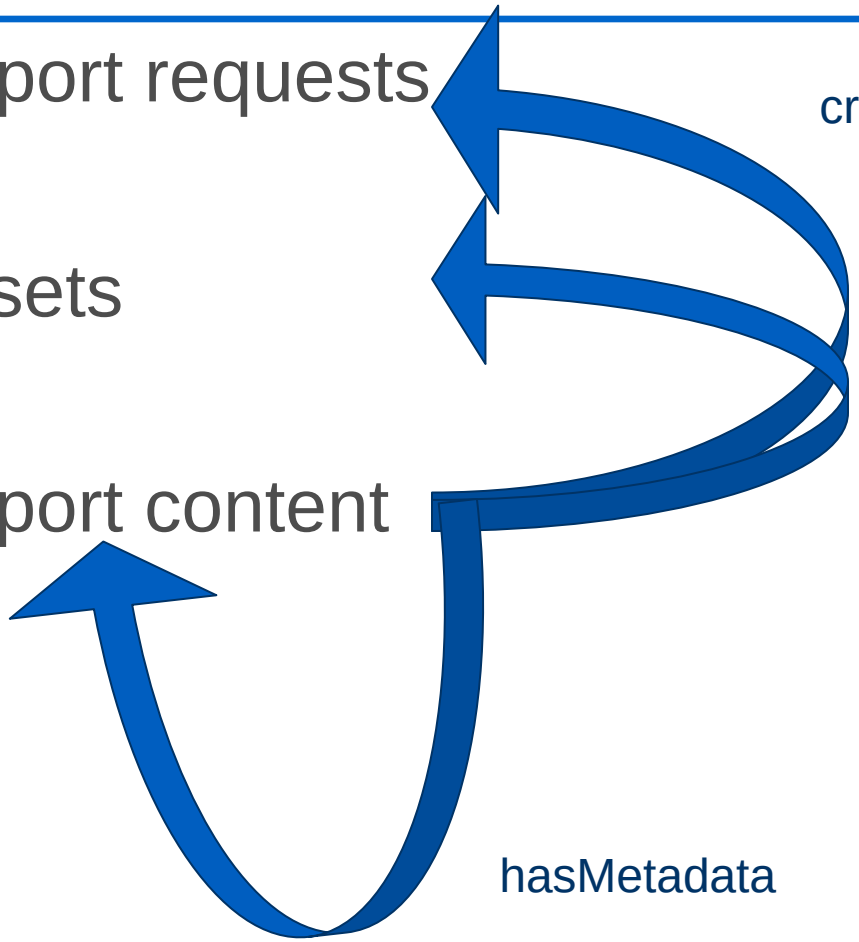
- Leverage the new Asset Reporting Format (ARF) – NIST IR 7694
- Enable stream based SCAP reporting
- Provide a well-defined output format for consumption in standard reporting tools
- Enable digital signing of result content

ARF Data Model Outline



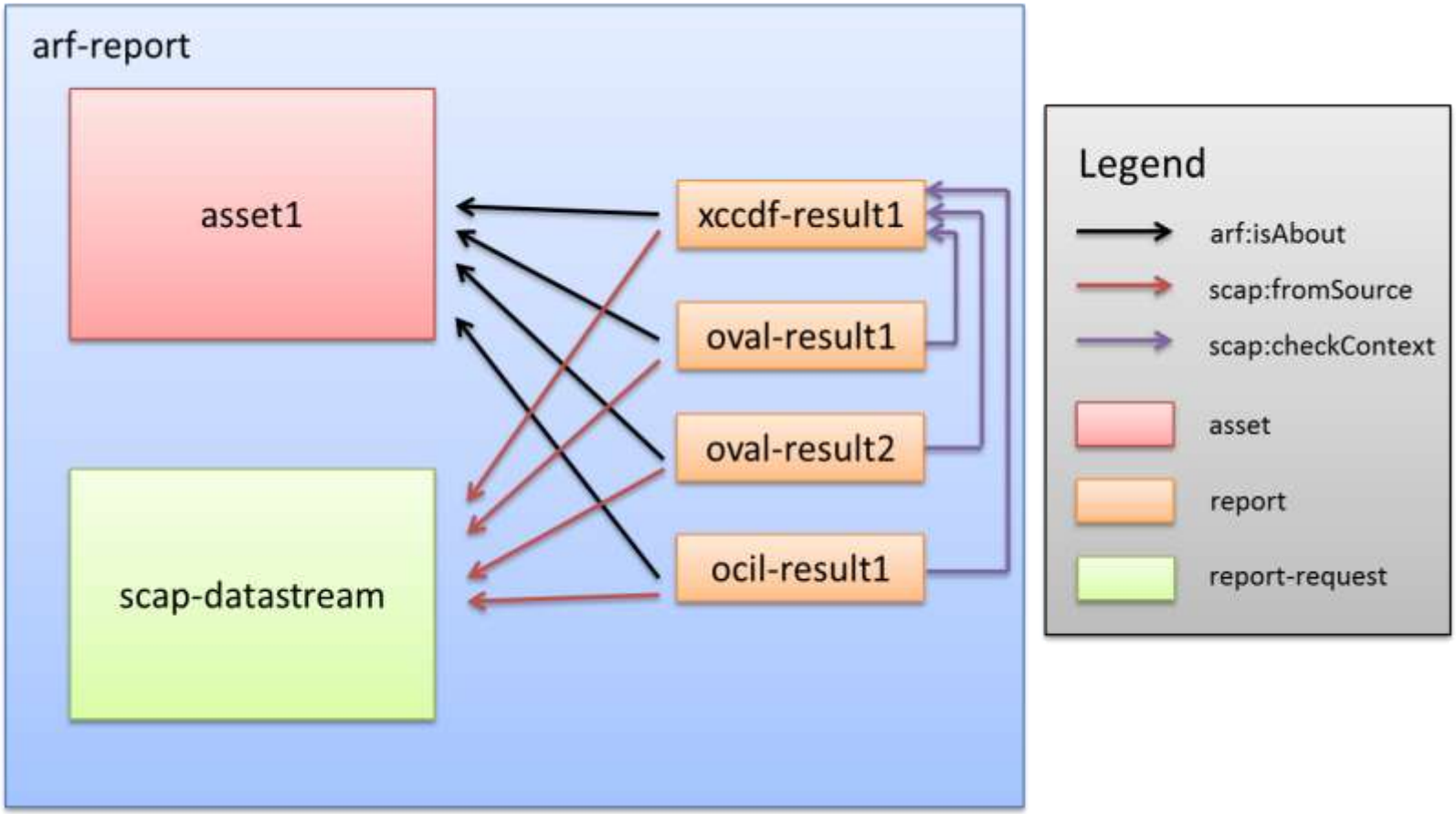
ARF: Objects To Be Related

- Report requests
- Assets
- Report content



http://scap.nist.gov/vocabulary/arf/relationships/1.0#

SCAP Result Data Stream Approach



Advantages

- Leverage the higher-level capabilities provided by ARF
- A report format that consolidates all SCAP results into a single XML file allows new capabilities such as web services
- Multiple results can be captured in a single report without replicating data
- The entire report can be signed

```
<asset-report-collection>
  <rc:relationships>
    <rc:relationship subject="minimal-xccdf-res.xml" type="rel:isAbout">
      <rc:ref>target1</rc:ref>
    </rc:relationship>
    <rc:relationship subject="minimal-oval-res.xml" type="rel:isAbout">
      <rc:ref>target1</rc:ref>
    </rc:relationship>
    <rc:relationship subject="minimal-cpe-oval-res.xml" type="rel:isAbout">
      <rc:ref>target1</rc:ref>
    </rc:relationship>
    <rc:relationship type="scap-rel:checkContext" subject="minimal-oval-res.xml">
      <rc:ref>minimal-xccdf-res.xml</rc:ref>
    </rc:relationship>
    <rc:relationship type="scap-rel:checkContext" subject="minimal-cpe-oval-res.xml">
      <rc:ref>minimal-xccdf-res.xml</rc:ref>
    </rc:relationship>
    <rc:relationship type="scap-rel:fromSource" subject="minimal-xccdf-res.xml">
      <rc:ref>scap-datastream1</rc:ref>
    </rc:relationship>
    <rc:relationship type="scap-rel:fromSource" subject="minimal-oval-res.xml">
      <rc:ref>scap-datastream1</rc:ref>
    </rc:relationship>
    <rc:relationship type="scap-rel:fromSource" subject="minimal-cpe-oval-res.xml">
      <rc:ref>scap-datastream1</rc:ref>
    </rc:relationship>
  </rc:relationships>
```

```
<report-requests>
    <report-request id="scap-datastream1">
      <scap:datastream-collection>
        ...
      </scap:datastream-collection>
    </report-request>
  </report-requests>
  <assets>
    <asset id="target1">
      <ai:computing-device>
        <ai:connections>
          <ai:connection>
            <ai:ip-address>
              <ai:ip-v4>127.0.0.1</ai:ip-v4>
              <ai:ip-v6>0:0:0:0:0:0:0:1</ai:ip-v6>
            </ai:ip-address>
          </ai:connection>
        </ai:connections>
        <ai:hostname>host.domain.tld</ai:hostname>
      </ai:computing-device>
    </asset>
  </assets>
```

```
<reports>
    <report id="minimal-xccdf-res.xml">
      <content>
        <xccdf:TestResult>
            ...
        </xccdf:TestResult>
      </content>
    </report>
    <report id="minimal-oval-res.xml">
      <content>
        <oval-res:oval_results>
            ...
        </oval-res:oval_results>
      </content>
    </report>
    <report id="minimal-cpe-oval-res.xml">
      <content>
        <oval-res:oval_results>
            ...
        </oval-res:oval_results>
      </content>
    </report>
  </reports>
</asset-report-collection>
```

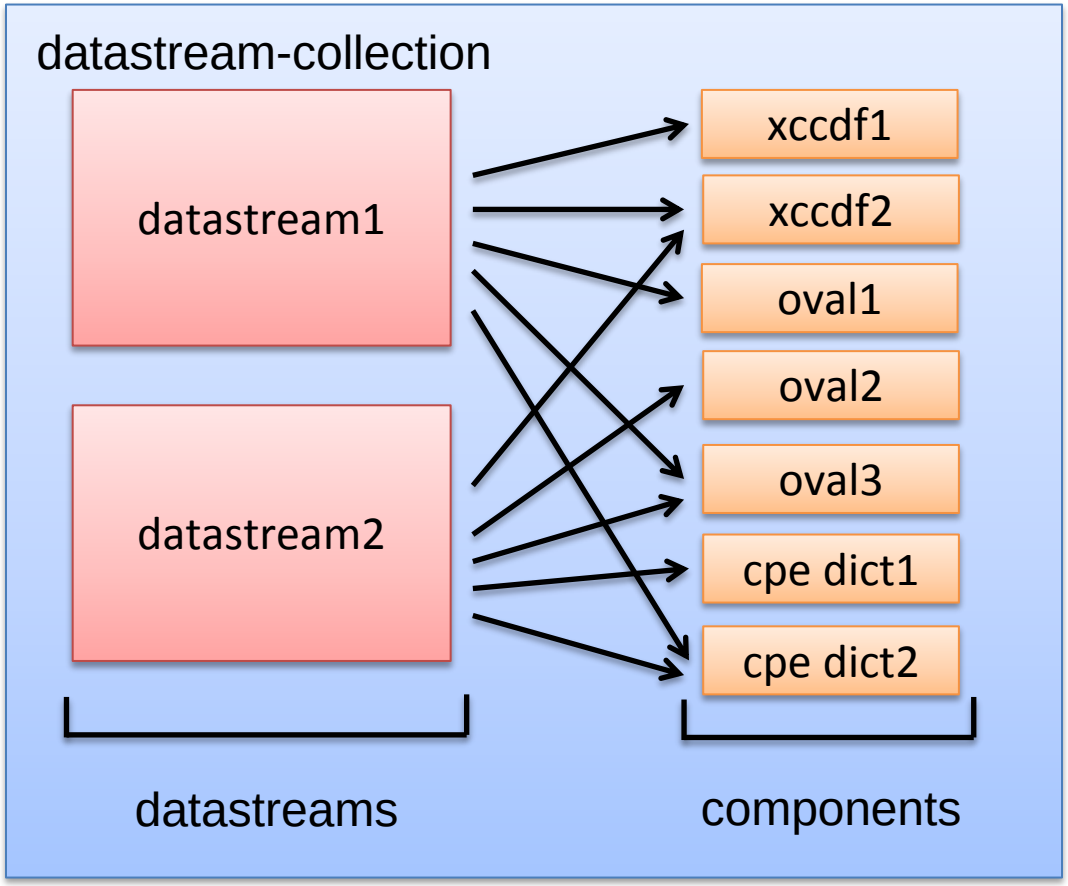
Agenda

- SCAP Source Data Stream
- SCAP Result Data Stream
- Signing SCAP Source Data Stream
- Signing SCAP Result Data Stream

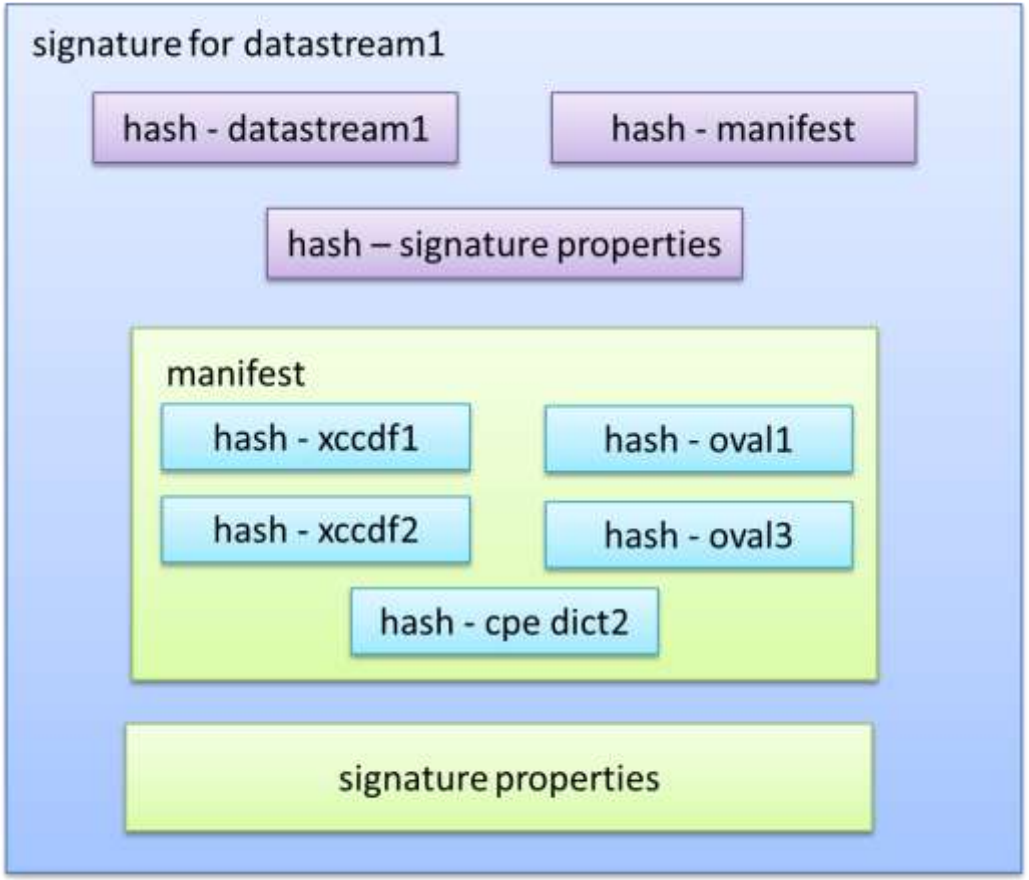
Introduction

- Objective
  - Optionally support data integrity in SCAP content by allowing digital signing of source content
- Requirements
  - Support W3C digital signatures for SCAP source data streams, in conformance with best practices
  - Comply with NIST guidance regarding digital signatures for security automation data (NIST IR 7802: Trust Model for Security Automation Data)

Approach – Data Stream Refresher



Approach - Signature



Advantages

- Each data stream and set of references can be individually signed, ensuring integrity for the individual parts of the data stream
- The signature and the references can be validated in different steps in the workflow (especially important for remote references)
- Components can be hashed once, and then reused without recomputing the hash every time

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="dsig-20111021162207939-77">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <Reference URI="#scap_gov.nist_datastream_Win7-54-1.2.0.0.zip">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>EmMJ6VoPw9RUD4sNrJbc1T480EbfLQMD2tggp/9VmUQ=</DigestValue>
    </Reference>
    <Reference Type="http://www.w3.org/2000/09/xmldsig#Manifest" URI="#manifest-20111021162207799-66">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>5N6jbIBlUTmXJB/PFIfQuUs1/GAnHWH2xazEMoWxfkk=</DigestValue>
    </Reference>
    <Reference Type="http://www.w3.org/2000/09/xmldsig#SignatureProperties" URI="#sig-prop-
20111021162207939-7">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>luwgMxaTQWajaSD9JfmsVvbgOSI6DzOg92Q63pMSBj4=</DigestValue>
    </Reference>
  </SignedInfo>
```

<SignatureValue>GcNr9O1IN3FiOSDdattsejYPSvFZ6Y9dDLZxWW/OJejhGyupL7BX2p7DQm+5KNPzT9i3JTNrBvi7
DcwLlaMOsaHTA9ka2Q9cGkaFW197FJV9D4Xv9e6fgToh0M/Ihf3z6+XPHtQxekFG74ZzoMAiQwbT
0efBB6cNwIIjpR9qKOPFsTS7Jk+LkGoJ1RRJZaGO940Mkm4RCfdGJTlRd7n6C+Bam3DrDROHRiNj
HMvkk7T64uBNUPmltgtFh38qUc+J8MfPCFnTS2K1YbrKE+xHtnKTHQyQxwrS0m566XepKSEQK2hT
rPLYGJty3p9uf6+X2MRzPCMYUjDYUN3JAweOlA==</SignatureValue>
<KeyInfo>
<KeyValue>
<RSAKeyValue>
<Modulus>z8adrX9m0S8OxIxN+fui33wiz4ZYgb4xPbR9MS5pOp1A8kVpH5Ew3N6O3/dMs2a4diIxyGLVh0r8
6QXWH/W6T2IC2ny+hi+jWRwXrvgTY3ZAFgePvz2OdRhVN/cUbOto4Pa4I2mVZWW+/Q0Fn7YpqPBD
DxlGq/xyFPuYq/4y7Y+Ah+vHO2ZSaiQjbj8F38XrGhwlcbFVyK8AmxK3z0zWwX86uMEqVCjW6s6j
2KAWdbAjEpgZHlJY87i/DqnFgxfmdg3oru+YeiEPVRY8hyQpYbtgryveZOHTgnCHmS/53U9jSS0c
yb/ADuj1upfyNoOiMMgQr7Olhc5pTvuWAl4Fnw==</Modulus>
<Exponent>AQAB</Exponent>
</RSAKeyValue>
</KeyValue>
</KeyInfo>

```
<Object>
  <Manifest Id="manifest-20111021162207799-66">
   <Reference URI="#scap_gov.nist_comp_USGCB-Windows-7-cpe-dictionary.xml">
    <Transforms>
     <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <DigestValue>L55GyzMwJrocb0/+sdYYESGZqrgi8XSGD/ZUY+xmrFY=</DigestValue>
   </Reference>
   <Reference URI="#scap_gov.nist_comp_USGCB-Windows-7-xccdf.xml">
    <Transforms>
     <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <DigestValue>txauWMRUUPFc8srAUjS9WDVWeIaetbxZrMTJYtQt1GA=</DigestValue>
   </Reference>
   <Reference URI="#scap_gov.nist_comp_USGCB-Windows-7-oval.xml">
    <Transforms>
     <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <DigestValue>wAE2d7fBRsiFfKCWK4BI1pPZtTTxz4220L+tWMrnm/o=</DigestValue>
   </Reference>
```

```
    <Reference URI="#scap_gov.nist_comp_USGCB-Windows-7-patches.xml">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>wH6zw8Pi0ThnZviPGKSKCnC2wLu9qgJZScC25z+v8do=</DigestValue>
    </Reference>
    <Reference URI="#scap_gov.nist_comp_USGCB-Windows-7-cpe-oval.xml">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>mYi3yOaeXhsMBa0bC+Gg/ZYkuOaCphV0pZ0C+6t5JpM=</DigestValue>
    </Reference>
   </Manifest>
  </Object>
  <Object>
   <SignatureProperties Id="sig-prop-20111021162207939-7">
    <SignatureProperty Target="#dsig-20111021162207939-77">
     <dsig:signature-info xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dsig="http://scap.nist.gov/schema/xml-
dsig/1.0">
      <dc:author>John Smith</dc:author>
       <dc:author>ACME Inc</dc:author>
       <dc:date>2011-10-21T16:22:07-0700</dc:date>
       <dsig:nonce>A7212381F3F10C1D</dsig:nonce>
      </dsig:signature-info>
    </SignatureProperty>
   </SignatureProperties>
  </Object>
 </Signature>
```

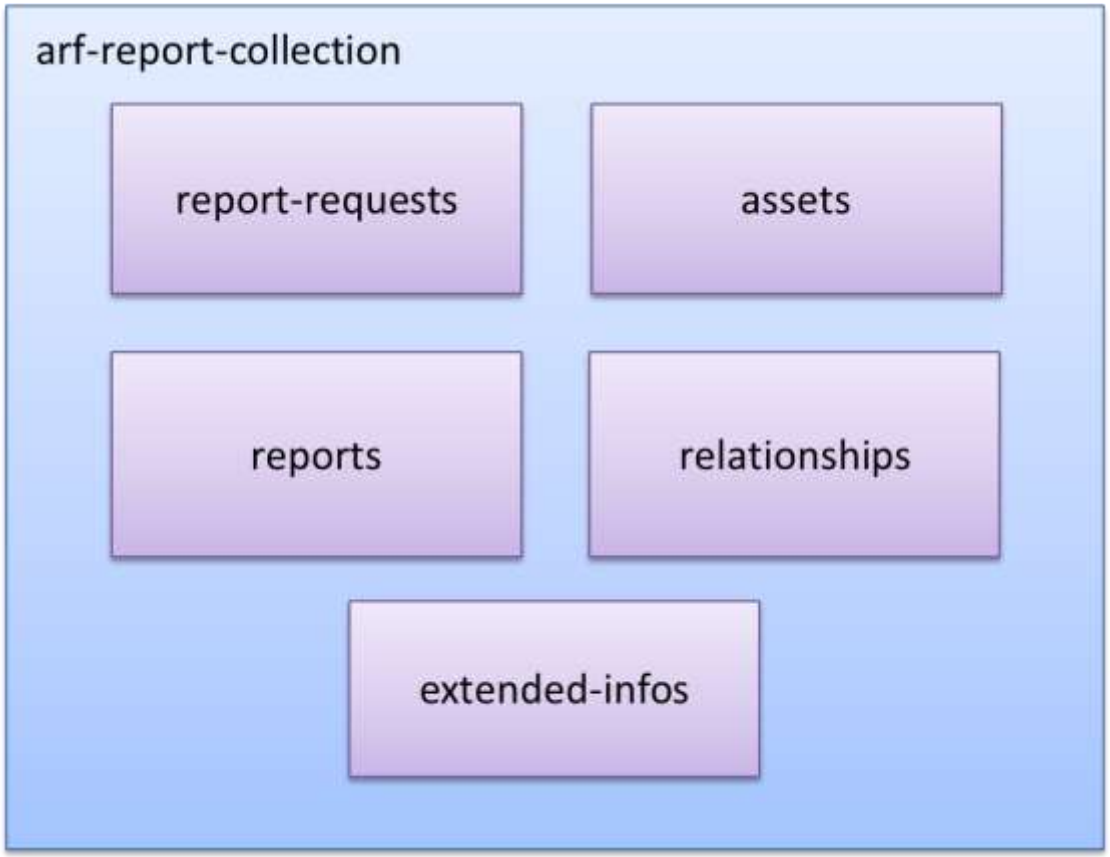
Agenda

- SCAP Source Data Stream
- SCAP Result Data Stream
- Signing SCAP Source Data Stream
- Signing SCAP Result Data Stream

Introduction

- Objective
  - Optionally support data integrity in SCAP result reports by allowing digital signing of the report
- Requirements
  - Support W3C digital signatures for SCAP result reports, in conformance with best practices
  - Comply with NIST guidance regarding digital signatures (NIST IR 7802: Trust Model for Security Automation Data)

Approach - ARF



Approach – ARF (Con't)

- Reference the parent asset-report-collection
- Exclude the extended-infos that have Signatures in them
  - /arf:asset-report-collection/arf:extended-infos[count(arf:extended-info[dsig:Signature]) = count(*)]
  - /arf:asset-report-collection/arf:extended-infos/arf:extended-info[dsig:Signature]

```
<extended-infos>
  <extended-info id="dsig-20111024081046011-94">
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="dsig-20111024081046226-17">
    <SignedInfo>
     <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
     <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
     <Reference URI="">
      <Transforms>
       <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
       <Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
        <XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2"
         xmlns:arf="http://scap.nist.gov/schema/asset-reporting-format/1.1"
         xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Filter="subtract"
         >/arf:asset-report-collection/arf:extended-infos[count(arf:extended-info[dsig:Signature]) =
         count(*)]</XPath>
        <XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2"
         xmlns:arf="http://scap.nist.gov/schema/asset-reporting-format/1.1"
         xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Filter="subtract"
         >/arf:asset-report-collection/arf:extended-infos/arf:extended-info[dsig:Signature]</XPath>
       </Transform>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>8gUMxUZiPYpUEzfKUq5H4EBfpmKiKcUBj+oeICc+cek=</DigestValue>
     </Reference>
     <Reference Type="http://www.w3.org/2000/09/xmldsig#SignatureProperties" URI="#sig-prop-20111024081046226-10">
      <Transforms>
       <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>TDaM60fl+3UreEfo4LLDm8itZ0XNZXpfFfN2fFSe9F0=</DigestValue>
     </Reference>
    </SignedInfo>
```

```
<SignatureValue>StIMZ2yyjFwe0lMq2IVCxoUTAcy0/8XZjTr5P6NvbRHoAw0zJM0NXrtCvVu7b/RzaBzFyfpx3hM0
      rsbTeyfSemMr3KZDKCi2ndL92xyHvR/jJ1e6QgEZu1p3QxjE3i5FlulYNToHL+mEJEWgKbpb0dQu
      nkfpCVmhLdnot1FW+bdk092b0z2JzZqhM8GTWCYMrhQ9ERH2MFGNNwqg9GpBgdggxiIMZ1t3/qgG
      GAVgZIe3eur8NOkZYpvd6paav0qcGfCENRzaxDcDnJJdA9iTf3eTgQ7IzryOJJRXjyJHlInBtTNC
      groAiMb3QAasHq2hEfAojWp3cksMoINkTZohrg==</SignatureValue>
    <KeyInfo>
     <KeyValue>
      <RSAKeyValue>
       <Modulus>z8adrX9m0S8OxIxN+fui33wiz4ZYgb4xPbR9MS5pOp1A8kVpH5Ew3N6O3/dMs2a4diIxyGLVh0r8
        6QXWH/W6T2IC2ny+hi+jWRwXrvgTY3ZAFgePvz2OdRhVN/cUbOto4Pa4I2mVZWW+/Q0Fn7YpqPBD
        DxlGq/xyFPuYq/4y7Y+Ah+vHO2ZSaiQjbj8F38XrGhwlcbFVyK8AmxK3z0zWwX86uMEqVCjW6s6j
        2KAWdbAjEpgZHlJY87i/DqnFgxfmdg3oru+YeiEPVRY8hyQpYbtgryveZOHTgnCHmS/53U9jSS0c
        yb/ADuj1upfyNoOiMMgQr7Olhc5pTvuWAl4Fnw==</Modulus>
       <Exponent>AQAB</Exponent>
      </RSAKeyValue>
     </KeyValue>
    </KeyInfo>
    <Object>
     <SignatureProperties Id="sig-prop-20111024081046226-10">
      <SignatureProperty Target="#dsig-20111024081046226-17">
       <dsig:signature-info xmlns:dc="http://purl.org/dc/elements/1.1/"
        xmlns:dsig="http://scap.nist.gov/schema/xml-dsig/1.0">
        <dc:author>John Smith</dc:author>
        <dc:author>ACME Inc</dc:author>
        <dc:date>2011-10-24T08:10:46-0700</dc:date>
        <dsig:nonce>7CAA36974FC26FD6</dsig:nonce>
       </dsig:signature-info>
      </SignatureProperty>
     </SignatureProperties>
    </Object>
   </Signature>
  </extended-info>
 </extended-infos>
```

Advantages

- Ensure integrity that the expected tool ran the content
- Enable a human-in-the-loop to certify the results
- Enable non-repudiation of result content

Resources

- SP 800-126 Rev 2 - The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2
- XML Schemas - http://scap.nist.gov/revision/1.2/index.html#schema
- Schematron rules - http://scap.nist.gov/revision/1.2/index.html#schematron

Questions & Answers / Feedback

Dave Waltermire (NIST)
david.waltermire@nist.gov - (301) 975-3390

Adam Halbardier (Booz Allen Hamilton)
Supporting NIST
adam.halbardier@nist.gov - (310) 297-5444

Karen Scarfone (Scarfone Cybersecurity/G2)
Supporting NIST
karen@scarfonecybersecurity.com - (703) 401-1018