TCG Infrastructure Working Group
Security Qualities Schema Specification

Specification Version 1.0
Revision 1.0
17 November 2006
FINAL

Contacts:
Paul_Sangster@symantec.com (Editor)
Ned.Smith@intel.com (Co-Chair)
thardjono@signacert.com (Co-Chair)
Disclaimer

THIS SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

No license, express or implied, by estoppel or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

Except that a license is hereby granted by TCG to copy and reproduce this specification for internal use only.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.
Acknowledgement

The TCG wishes to thank all those who contributed to this specification. This document builds on considerable work done in the various working groups in the TCG.

Special thanks to the members of the IWG contributing to this document:

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malcolm Duncan</td>
<td>CESG</td>
</tr>
<tr>
<td>Kazuaki Nimura</td>
<td>Fujitsu Limited</td>
</tr>
<tr>
<td>Diana Arroyo</td>
<td>IBM</td>
</tr>
<tr>
<td>Lee Terrell</td>
<td>IBM</td>
</tr>
<tr>
<td>Ned Smith (co-chair)</td>
<td>Intel</td>
</tr>
<tr>
<td>Greg Kazmierczak</td>
<td>Wave Systems</td>
</tr>
<tr>
<td>Len Veil</td>
<td>Wave Systems</td>
</tr>
<tr>
<td>Paul Sangster (Editor)</td>
<td>Symantec</td>
</tr>
<tr>
<td>Willys Ingersoll</td>
<td>Sun Microsystems</td>
</tr>
<tr>
<td>Jeff Nisewanger</td>
<td>Sun Microsystems</td>
</tr>
<tr>
<td>Thomas Hardjono (co-chair)</td>
<td>SignaCert</td>
</tr>
</tbody>
</table>
# Table of Contents

1 Scope and Audience ................................................................. 6

2 Introduction ............................................................................ 7
   2.1 Normative Specification Content ........................................ 7
   2.2 Schema Version ............................................................... 7
   2.3 Schema Namespace ........................................................... 7
   2.4 Dependent Schema Definitions .......................................... 7
      2.4.1 W3C XML Schema Syntax ........................................ 7
      2.4.2 W3C XML-Signature Syntax ...................................... 8
      2.4.3 TCG Core Integrity Schema Syntax ............................... 8
      2.4.4 Schema Diagrams Conventions .................................... 8
      2.4.5 Keywords ................................................................. 8

3 Security Qualities Schema .................................................... 9
   3.1 Complex Types and Elements ............................................ 9
      3.1.1 complexType AdditionalInfoType ................................. 9
      3.1.2 complexType CommonCriteriaType .............................. 11
      3.1.3 element CommonCriteriaType/AssuranceLevel .................. 12
      3.1.4 element CommonCriteriaType/ProfileLocation .................. 13
      3.1.5 element CommonCriteriaType/TargetLocation .................. 14
      3.1.6 element CommonCriteriaType/VerificationReport ............... 15
      3.1.7 element CommonCriteriaType/CertificationBody ............... 17
      3.1.8 element CommonCriteriaType/AdditionalInfo ................... 17
      3.1.9 complexType FipsLevelType ........................................ 18
      3.1.10 element FipsLevelType/AdditionalInfo .......................... 20
      3.1.11 complexType Iso9000Type .......................................... 23
      3.1.12 element Iso9000Type/AdditionalInfo ............................. 24
      3.1.13 complexType SecurityQualitiesType .............................. 25

4 References ........................................................................... 27
1 Scope and Audience

This specification is integral to the TCG Infrastructure Working Group’s (IWG) reference architecture, and is directly related to the TCG’s Integrity Management Model. Specifically, the Security Qualities XML schema defines the structure with which claims about the security provided by a system can be asserted to other parties (e.g. relying parties.)

Architects, designers, developers, and technologists interested in the development, deployment, and interoperation of trusted systems will find this document necessary in providing a specific mechanism for communicating integrity information.
2 Introduction
This document defines the contents and format of the Security Qualities Schema. This schema is designed to be used within other schemas (such as the Reference Manifest schema [1]) to assert qualities of the component that might affect the verifier's decision making process about whether to trust the operation of the component. These qualities generally are not subject to direct (cryptographic) measurement so this allows the qualities to be asserted by a manufacturer and verified by relying parties in conjunction with component measurements.

The goal of this schema is to house security qualities which are associated with a component. For example, this allows for the creation of a single Reference Manifest to assert that a particular TPM (specific: make, model, firmware version) has been Common Criteria evaluated and describe the circumstances and results of the review. This manifest containing the assertions could be referenced by each platform that includes this TPM and thus asserts to offer the security qualities. These assertions are designed to be associated with a Reference Manifest using the AssertionInfo element.

While this schema intends to offer a rich set of information that might reflect the quality and thus trustworthiness of a component, it is expected that deployers may wish to associate a different set of information. This is possible using the AdditionalInfo element described below or by including a custom assertion schema (instead of this one) on the Reference Manifest's AssertionInfo element.

2.1 Normative Specification Content
The contents of this document should be considered to be NORMATIVE except for the XML schemas and associated structural diagrams. For XML schemas, the XML in this document is generated from the XSD files. While it is the intention of the authors to keep these representations consistent, the XSD files are considered NORMATIVE for all XML and any XML representations in this document are INFORMATIVE.

2.2 Schema Version
The Security Qualities schema’s version number is defined using the version attribute of the schema’s root-level schema element:

\[ \text{version=“version\_number”} \]

This document refers to version 1.00 of the Security Qualities schema.

2.3 Schema Namespace
The Security Qualities schema’s namespace is defined using the targetNamespace attribute of the schema’s root-level schema element:

\[ \text{targetNamespace=“namespace”} \]

The schema’s namespace reflects the schema version, and is currently defined as follows:

http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_0#

2.4 Dependent Schema Definitions
2.4.1 W3C XML Schema Syntax
The Security Qualities schema relies upon data structures defined by the World Wide Web Consortium’s (W3C) XML-Schema syntax. Consequently, the Reference Manifest schema imports the W3C’s XML schema with the following namespace:

http://www.w3.org/2001/XMLSchema
The Security Qualities schema associates the abovementioned schema with the “xs” namespace prefix.

### 2.4.2 W3C XML-Signature Syntax

The Security Qualities schema relies upon data structures defined by the World Wide Web Consortium’s (W3C) XML-Signature digital signature syntax. Consequently, the Security Qualities schema imports the W3C’s digital signature XML schema with the following namespace:

http://www.w3.org/2000/09/xmldsig#

The Security Qualities schema associates the abovementioned schema with the “ds” namespace prefix.

### 2.4.3 TCG Core Integrity Schema Syntax

This Security Qualities schema relies upon data structures defined by the TCG Core Integrity Schema Syntax, [1]. Consequently, this schema imports the TCG Core Integrity Schema with the following namespace:

http://www.trustedcomputinggroup.org/XML/SCHEMA/Core_Integrity_v1_0_1#

The Security Qualities schema associates the above mentioned schema with the “core” namespace prefix.

### 2.4.4 Schema Diagrams Conventions

The schema diagrams in this specification contain attributes and elements that are either mandatory or optional to populate. Those that are mandatory to populate are depicted by solid lines surrounding the attributes and elements. Those that are optional to populate are depicted by dashed lines surrounding the attributes and elements.

### 2.4.5 Keywords

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [11]. This specification does not distinguish blocks of informative comments and normative requirements. Therefore, for the sake of clarity, note that lower case instances of must, should, etc. do not indicate normative requirements.
3 Security Qualities Schema

The following are the complex types defined within this specification.

Complex types
- AdditionalInfoType
- CommonCriteriaType
- FipsLevelType
- Iso9000Type
- SecurityQualitiesType

3.1 Complex Types and Elements

3.1.1 complexType AdditionalInfoType

3.1.1.1 Description
The AdditionalInfo complex type provides a generic structure for pointing to a web document describing a security property that is embodied by the associated component. For example, this enables a manufacturer to associate a security property with a component (software, firmware or hardware) not covered by the other complex types described in this schema. Similarly, this type may be used by an IT department or any other party in the supply or deployment chain to bind information that might reflect the quality or trustworthiness of the component (e.g. IT compliance report.)

The AdditionalInfo type includes a generic URI that points to the document describing the security qualities asserted by the documents creator and a set of hash values of the document enabling relying parties to detect if the document is identical to the version when this assertion was created. The support for multiple hash values was included to allow for multiple digest algorithms to be used in parallel (e.g. URI's content is digested both in SHA-1 and SHA-256.) Finally a description of the quality can be included to aid a verifier's understanding of the context of the generic quality being asserted.
3.1.1.2 Diagram

```xml
<xs:complexType name="AdditionalInfoType">
  <xs:complexContent>
    <xs:extension base="core:HashedURIType">
      <xs:attribute name="Description" type="xs:string"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

namespace http://www.trustedcomputinggroup.org/XML/SCHHEMA/Security_Qualities_v1_0#

type extension of core:HashedURIType

properties base Core:HashedURIType

children `UriHash` CommonCriteriaType/AdditionalInfo

used by elements FipsLevelType/AdditionalInfo

Iso9000Type/AdditionalInfo

SecurityQualitiesType/AdditionalInfo

CommonCriteriaType/CertificateBody

CommonCriteriaType/ProfileLocation

CommonCriteriaType/TargetLocation

CommonCriteriaType/VerificationReport

attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Use</th>
<th>Default</th>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>xs:anyURI</td>
<td>required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>xs:string</td>
<td>optional</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.1.1.3 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>Reference to a web document describing the security quality to be associated with the component.</td>
</tr>
<tr>
<td>Description</td>
<td>Textual description of the context of the security quality asserted in the document to aid the verifier’s understanding of this generic field. This allows humans involved in the trust decision to understand the role of the document referenced by the URI since this can point to a wide range of types of documents.</td>
</tr>
</tbody>
</table>

3.1.1.4 XML

```xml
<xs:complexType name="AdditionalInfoType">
  <xs:complexContent>
    <xs:extension base="core:HashedURIType">
      <xs:attribute name="Description" type="xs:string"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```
3.1.2 complexType CommonCriteriaType

3.1.2.1 Description
The CommonCriteriaType complex type is a collection of information describing the security aspects ("qualities") of the associated component involved in a common criteria evaluation. This allows manufacturers to assert whether the component's evaluation was completed, is currently in progress or was built consistent with the evaluation criteria but no evaluation has occurred and any details associated with the process. For example, this type might contains references to the protection profile applied, evaluation results and the available supporting documentation which provides the context for how the component operates within the evaluated configuration. Information about the certifying body is included in case their sphere of influence affects the trust decisions. For more information on the common criteria evaluation process see [7].

3.1.2.2 Diagram
3.1.2.3 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version of the common criteria evaluation process used [6]. For example, version “2.3” of the common criteria process [7] is currently being used at the writing of this specification but version “3.0” was recently made public for comments.</td>
</tr>
<tr>
<td>EvaluationStatus</td>
<td>Current status of the component as it progresses through the common criteria evaluation process (even if the component was merely designed to meet the criteria but isn’t actually being evaluated.) This attribute allows for asserting that a product was: designed to meet (but not evaluated), currently being evaluated, or has completed evaluation and received the asserted assurance level.</td>
</tr>
<tr>
<td>CertificationDate</td>
<td>Date when product received its common criteria evaluation. This attribute should only be included when Evaluation Status is EvaluationCompleted.</td>
</tr>
</tbody>
</table>

3.1.2.4 XML

```xml
<xs:complexType name="CommonCriteriaType">
  <xs:sequence>
    <xs:element name="AssuranceLevel">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:integer">
            <xs:attribute name="StrengthOfFunction" use="optional">
              <xs:simpleType>
                <xs:restriction base="xs:NMTOKEN">
                  <xs:enumeration value="Basic"/>
                  <xs:enumeration value="Medium"/>
                  <xs:enumeration value="High"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
            <xs:attribute name="Plus" type="xs:boolean"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
      <xs:attribute name="Version" type="xs:normalizedString" use="required"/>
      <xs:attribute name="EvaluationStatus" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="DesignedToMeet"/>
            <xs:enumeration value="EvaluationInProgress"/>
            <xs:enumeration value="EvaluationCompleted"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
      <xs:attribute name="CertificationDate" type="xs:date"/>
    </xs:element>
    <xs:element name="ProfileLocation" type="AdditionalInfoType" minOccurs="0"/>
    <xs:element name="TargetLocation" type="AdditionalInfoType" minOccurs="0"/>
    <xs:element name="VerificationReport" type="AdditionalInfoType" minOccurs="0"/>
    <xs:element name="CertificationBody" type="AdditionalInfoType" minOccurs="0"/>
    <xs:element name="AdditionalInfo" type="AdditionalInfoType" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
```

3.1.3 element CommonCriteriaType/AssuranceLevel

3.1.3.1 Description

This element captures the result (or anticipated result) of the Common Criteria evaluation. The result contains an overall assurance level that the evaluator believed the component achieved. This value reflects only the numeric portion of the EAL expression and must be within a range of...
1 to 7 inclusive. For example, a component might achieve an “EAL4” assurance level (represented as just a “4” in the AssuranceLevel element.) If the assurance level received is “EAL4+” this would also require the use of the Plus boolean attribute.

```
<xs:element name="AssuranceLevel">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="xs:integer">
        <xs:attribute name="StrengthOfFunction" use="optional">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="Basic"/>
              <xs:enumeration value="Medium"/>
              <xs:enumeration value="High"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="Plus" type="xs:boolean"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
```

3.1.3.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StrengthOfFunction</td>
<td>Level of robustness of the function of the component (e.g. “medium”). If the evaluation result includes a strength of function, then it must be expressed using this attribute. If this attribute is not expressed, then the verifier should assume that no such strength of function was part of the evaluation result.</td>
</tr>
<tr>
<td>Plus</td>
<td>Additional indicator that the product went beyond the indicated assurance level.</td>
</tr>
</tbody>
</table>

3.1.3.3 XML

```
<xs:element name="AssuranceLevel">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="xs:integer">
        <xs:attribute name="StrengthOfFunction" use="optional">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="Basic"/>
              <xs:enumeration value="Medium"/>
              <xs:enumeration value="High"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="Plus" type="xs:boolean"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
```

3.1.4 element CommonCriteriaType/ProfileLocation

3.1.4.1 Description

This element is a reference to the location of the protection profile description. The protection profile describes the security context which the component was evaluated against in a non-product specific manner. In order to prevent tampering with the protection profile description, this element includes a cryptographic hash of its contents. Verifiers can use this to detect changes to the profile after this assertion was generated (e.g. possibly including additional security properties that were not part of this evaluation) that potentially affect its trust decision.
### 3.1.4.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>Location of the protection profile document expressed in URI format.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the referenced protection profile document.</td>
</tr>
</tbody>
</table>

### 3.1.4.3 XML

```xml
<xs:element name="ProfileLocation" type="AdditionalInfoType" minOccurs="0"/>
```

### 3.1.5 element CommonCriteriaType/TargetLocation

#### 3.1.5.1 Description

This element references the security target document used as the basis of the evaluation of the component. This document normally covers the security characteristics of the component being evaluated including important information about the security requirements met by the component and how the component may be used and remain within the context of the Common Criteria evaluation. While the security target is normally specific to a particular vendor's component, it frequently is based upon or references a product neutral protection profile when an appropriate profile exists. This document is commonly made available and contains information essential to the verifier's understanding of the security provided by the component.
3.1.5.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to the security target (unstructured) document. This is available for humans to consider whether the intended use of the component is consistent with its evaluation. The result of this consideration might be stored by a verifier to avoid repeated human intervention when the same component is used in future transactions.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the security target document being referenced.</td>
</tr>
</tbody>
</table>

3.1.6 element CommonCriteriaType/VerificationReport

3.1.6.1 Description

This element provides a reference to a document known as a Certification or Verification Report that describes in more detail the context of the component’s evaluation and the final results. Since the verifier should consider these detailed findings (in conjunction with the security target), it is important that the integrity of the report be protected from change after the assertion reference is created (e.g. to detect an adversary including false results.) The included hash(es) allows the verifier to detect changes in the document.
3.1.6.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to the verification report created by the certifying body as a result of the evaluation. The verification report is an unstructured document intended to be consumed by a human. The contents may affect the level of confidence a verifier has in the use of this type of component.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable Information about the verification report referenced by UriValue.</td>
</tr>
</tbody>
</table>

3.1.6.3 XML

```xml
<xs:element name="VerificationReport" type="AdditionalInfoType" minOccurs="0"/>
```
3.1.7 element CommonCriteriaType/CertificationBody

3.1.7.1 Description
This element references information about the certification body that performed the evaluation as per the rules of the Common Criteria process. Depending on the country of operation of the verifier, the country associated with the certifying body and the resulting assurance level may affect its trustworthiness. For example, assurance levels above EAL4+ may not be recognized by verifiers in countries outside of the nation which performed the evaluation.

![Diagram]

namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_0#
type AdditionalInfoType

3.1.7.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted location of a web page or document which describes the certifying body which performed the evaluation of the component.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the document referenced by UriValue.</td>
</tr>
</tbody>
</table>

3.1.7.3 XML

```
<xs:element name="CertificationBody" type="AdditionalInfoType" minOccurs="0"/>
```

3.1.8 element CommonCriteriaType/AdditionalInfo

3.1.8.1 Description
This element provides for a general description of information about the component's common criteria evaluation process or results. For example, this might include a reference to an on-line certificate image issued by a member of the International Common Criteria Mutual Recognition Arrangement (ICCMRA.) Because this element is generic it is particularly beneficial to include a human readable description of the purpose of the reference within this type. This element should
not be used for referencing information applicable to one of the other elements of CommonCriteriaType complex type.

3.1.8.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to a web page or document describing some aspect of the evaluation or result not associated with one of the other elements of CommonCriteriaType.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the purpose of the referenced document. Because this is a general purpose reference this description is particularly helpful for the person reviewing the evaluation qualities.</td>
</tr>
</tbody>
</table>

3.1.8.3 XML

```xml
<xs:element name="AdditionalInfo" type="AdditionalInfoType" minOccurs="0"/>
```

3.1.9 complexType FipsLevelType

3.1.9.1 Description

This element captures the results of a NIST FIPS evaluation of the component. Such an evaluation may focus on the security boundary of the cryptography included in the component (e.g. FIPS 140.) This schema is designed to capture information about the overall result (Level), the lab performing the test (TestLab), the security properties asserted by the component’s vendor (SecurityPolicy) and which of these properties were observed by the testing lab (TestReport.)

In the FIPS 140-2 world, the independent verification testing labs are accredited by the CMT (Cryptographic Module Testing) laboratories of the US NIST (National Institute for Standards and Technology) and the Canadian CSE (Communications Security Establishment.) to perform the testing of the security policies and to generate a test report. This report forms the basis for
determining if the component meets the requirements for a 140-2 certification. This type allows for each of these documents and entities to be defined so that a verifier may factor this information into its decision.

```xml
<xs:complexType name="FipsLevelType">
  <xs:sequence minOccurs="0">
    <xs:element name="AdditionalInfo" type="AdditionalInfoType"/>
    <xs:element name="SecurityPolicy" type="AdditionalInfoType"/>
    <xs:element name="TestReport" type="AdditionalInfoType"/>
    <xs:element name="TestingLab" type="AdditionalInfoType"/>
  </xs:sequence>
  <xs:attribute name="Specification" type="xs:normalizedString" use="required"/>
  <xs:attribute name="Level" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:integer"/>
    </xs:simpleType>
  </xs:attribute>
</xs:complexType>
```

3.1.9.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification</td>
<td>Identification of which FIPS standards was applied for the evaluation. It’s envisioned that this would be used for at least representing FIPS 140 evaluations. For example, this attribute might be “140-2”</td>
</tr>
<tr>
<td>Level</td>
<td>Result of the FIPS evaluation (e.g. “Level 2” would be represented as just “2”.) This value must be in the inclusive range of 1-4 which are the recognized evaluation levels for FIPS 140-1 and 140-2 products.</td>
</tr>
</tbody>
</table>

3.1.9.3 XML

```xml
<xs:complexType name="FipsLevelType">
  <xs:sequence minOccurs="0">
    <xs:element name="AdditionalInfo" type="AdditionalInfoType"/>
    <xs:element name="SecurityPolicy" type="AdditionalInfoType"/>
    <xs:element name="TestReport" type="AdditionalInfoType"/>
    <xs:element name="TestingLab" type="AdditionalInfoType"/>
  </xs:sequence>
  <xs:attribute name="Specification" type="xs:normalizedString" use="required"/>
  <xs:attribute name="Level" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:integer"/>
    </xs:simpleType>
  </xs:attribute>
</xs:complexType>
```
3.1.10 element FipsLevelType/SecurityPolicy

3.1.10.1 Description
This element provides a reference to the Security Policy document associated with the component. This document describes the proper operation and environment for use of the component and the (normally) vendor claimed security properties exhibited. This document is useful to the verifier to understand how the component should be used within a platform and thus may factor this information into the trust decision when evaluating how the component is in fact being used by the other party (e.g. how its described within a Verification Report.) It is not envisioned that this level of detail will be required for all verifiers and some vendors may not wish to publish such a document so this element is left optional in the schema.

```
<xs:element name="SecurityPolicy" type="AdditionalInfoType"/>
```

3.1.10.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to the Security Policy document. This includes information potentially useful to the verifier to understand the claimed security properties of the component.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the referenced Security Policy document. This is useful to humans involved with the verification process attempting to analyze the trustworthiness of a component.</td>
</tr>
</tbody>
</table>

3.1.10.3 XML

```
<xs:element name="SecurityPolicy" type="AdditionalInfoType"/>
```
### 3.1.11 element FipsLevelType/TestReport

#### 3.1.11.1 Description
This element provides a protected reference to the final verification test report by the NVLAP accredited lab describing the testing performed and the results observed. This report includes a lot of detail that might be of interest to sophisticated verifiers who wish more information than the overall result (whether it passed and the achieved level.)

![Diagram](image)

**namespace** http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_0#

**type** AdditionalInfoType

**properties**
- **isRef**: 0
- **content**: complex

**children**
- UriHash

**attributes**
- **Name**: Type xs:string, Use required, Default Fixed
- **UriValue**: Type xs:anyURI, Use required
- **Description**: Type xs:string, Use optional

#### 3.1.11.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to the test report associated with the associated component.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the test results document. This is useful to humans involved with the verification process attempting to analyze the trustworthiness of a component.</td>
</tr>
</tbody>
</table>

#### 3.1.11.3 XML

```
<xs:element name="TestReport" type="AdditionalInfoType"/>
```

### 3.1.12 element FipsLevelType/TestingLab

#### 3.1.12.1 Description
This element includes a reference to a document describing the NVLAP accredited CMT lab involved with the certification of this component. This information might be useful for verifiers that do not wish to trust equally all of the accredited labs findings (e.g. for geo-political reasons) despite the NIST/CVE issuing the certification of the component.
3.1.12.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to an available document describing the laboratory that performed the validation testing on the component.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the purpose of the referenced document. This is useful to humans involved with the verification process attempting to analyze the trustworthiness of a component.</td>
</tr>
</tbody>
</table>

3.1.12.3 XML

```xml
<xs:element name="TestingLab" type="AdditionalInfoType"/>
```

3.1.13 element FipsLevelType/AdditionalInfo

3.1.13.1 Description

This element allows for the association of other information about the FIPS evaluation not covered by the other FIPS-related elements. This enables a reference to be included to a document describing more information about the evaluation process, result or environmental constraints necessary to sustain the evaluation rating. Another possible use of this type would be to directly reference an on-line copy of the physical certificate issued by NIST for this component.
3.1.13.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to an available document describing some aspect of the FIPS evaluation process of the component.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the purpose of the referenced document. This is useful to humans involved with the verification process attempting to analyze the trustworthiness of a component.</td>
</tr>
</tbody>
</table>

3.1.13.3 XML

```xml
<source>
  <xs:element name="AdditionalInfo" type="AdditionalInfoType"/>
</source>
```

3.1.14 complexType Iso9000Type

3.1.14.1 Description

This complex type describes the type of ISO 9000 [8] conformance and evaluation that was performed on the component’s design and development environment and whether it was considered compliant.
3.1.14.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpecName</td>
<td>Name (including year version) of the ISO 9000 specification which was used as the basis for the evaluation of the environment used to design and build the component. For example, this could be represented as &quot;ISO 9000:2000&quot; if this version of the ISO 9000 specification was used.</td>
</tr>
<tr>
<td>IsCompliant</td>
<td>Boolean result of whether the environment used to design and build the component met the associated ISO 9000 criteria.</td>
</tr>
</tbody>
</table>

3.1.14.3 XML

```xml
<xs:complexType name="Iso9000Type">
    <xs:sequence minOccurs="0">
        <xs:element name="AdditionalInfo" type="AdditionalInfoType"/>
    </xs:sequence>
    <xs:attribute name="SpecName" type="xs:NMTOKEN" use="required"/>
    <xs:attribute name="IsCompliant" type="xs:boolean"/>
</xs:complexType>
```

3.1.15 element Iso9000Type/AdditionalInfo

3.1.15.1 Description

This element allows for the addition of information not described by the other elements tied to ISO 9000 evaluation above. This might include information about the ISO 9000 compliance process that was the focus on the evaluation and information about the results of the evaluation including when it took place and how often re-evaluations are expected to occur.
3.1.15.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UriValue</td>
<td>URI formatted reference to a document describing more information about the application of the ISO 9000 evaluation processes or results associated with the component.</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of the referenced document.</td>
</tr>
</tbody>
</table>

3.1.15.3 XML

```xml
<xs:element name="AdditionalInfo" type="AdditionalInfoType"/>
```

3.1.16 complexType SecurityQualitiesType

3.1.16.1 Description

This type allows for the definition of the security properties asserted to be associated with the component. These qualities generally can not be measured by hashing some aspect of the component and must be asserted by a trustworthy party. This type houses a wide variety of types of security properties (qualities) generally associated with processes and results tied to an evaluation of the component performed by a trusted, widely recognized 3rd party.

```
namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_0#
```
3.1.16.2 Attribute Detail

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

3.1.16.3 XML

```xml
<xs:complexType name="SecurityQualitiesType">
  <xs:sequence>
    <xs:element name="CommonCriteria" type="CommonCriteriaType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="FipsLevel" type="FipsLevelType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="Iso9000" type="Iso9000Type" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="AdditionalInfo" type="AdditionalInfoType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="DigestMethod" type="core:DigestMethodType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="Transforms" type="core:TransformMethodType" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
```
4 References


