

TCG Infrastructure Working Group Security Qualities Schema

**Specification Version 1.1
Revision 7
21 May 2007
Published**

Contacts:
admin@trustedcomputinggroup.org

TCG PUBLISHED

Copyright © TCG 2007

TCG

Copyright © 2007 Trusted Computing Group, Incorporated.

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.

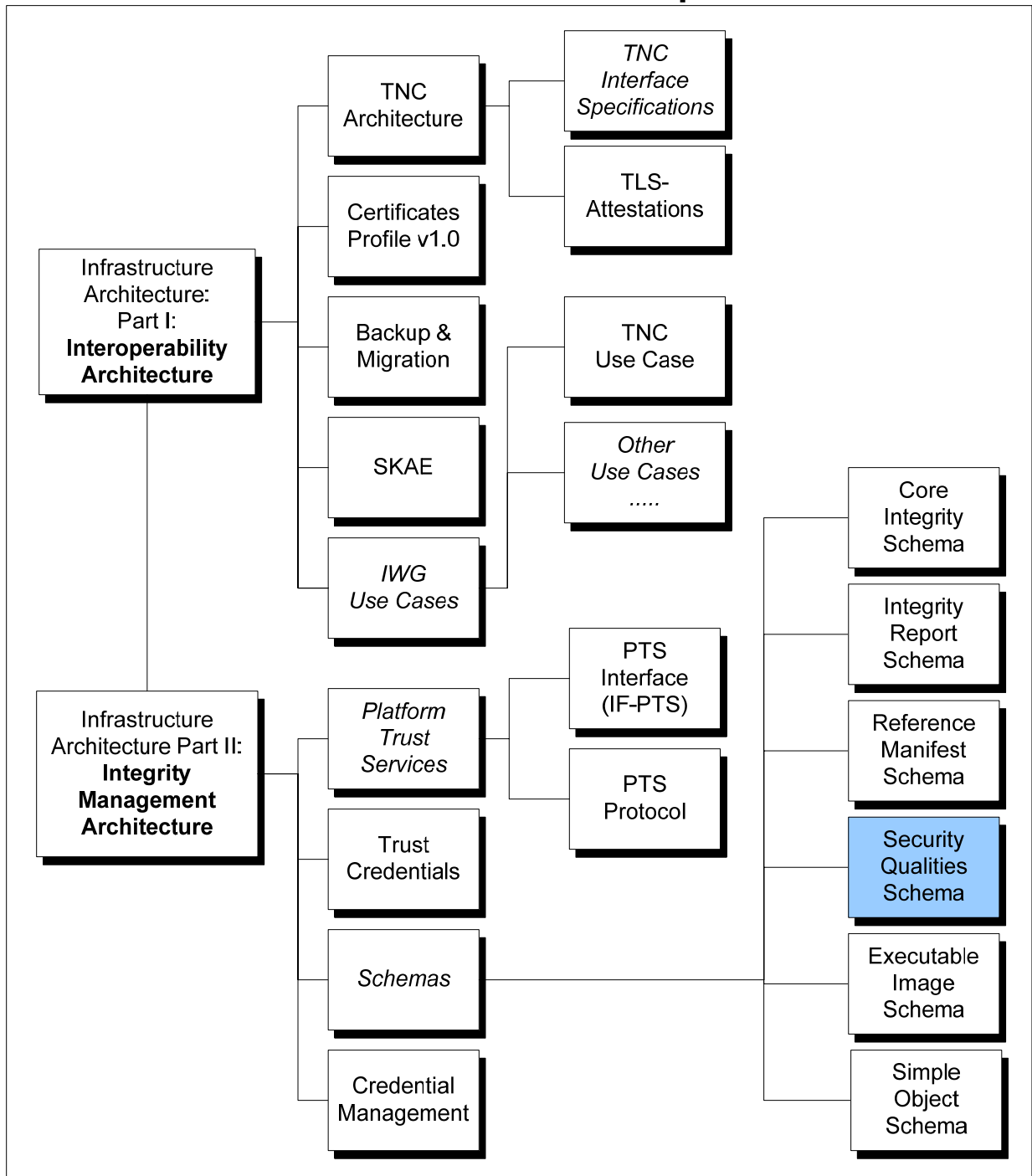
No license, express or implied, by estoppel or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

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.

IWG Document Roadmap



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:

Malcolm Duncan	CESG
Kazuaki Nimura	Fujitsu Limited
Diana Arroyo	IBM
Lee Terrell	IBM
Ned Smith (IWG co-chair)	Intel
Sandi Roddy	NSA
Wyllys Ingersoll	Sun Microsystems
Jeff Nisewanger	Sun Microsystems
Paul Sangster (Editor)	Symantec Corporation
Thomas Hardjono (IWG co-chair)	Wave Systems
Greg Kazmierczak	Wave Systems
Len Veil	Wave Systems

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	8
2.4.1	W3C XML Schema Syntax.....	8
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/SecurityPolicy	20
3.1.11	element FipsLevelType/TestReport	21
3.1.12	element FipsLevelType/TestingLab	21
3.1.13	element FipsLevelType/AdditionalInfo	22
3.1.14	complexType Iso9000Type	23
3.1.15	element Iso9000Type/AdditionalInfo.....	24
3.1.16	complexType TPMSecurityAssertionsType	25
3.1.17	complexType TBBSecurityAssertionsType	27
3.1.18	complexType SecurityQualitiesType.....	28
4	References.....	31

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.

Version 1.1 of this specification includes assertions made about the TPM and TBB in the TCG Credentials 1.0 specification[9]. This enables the security qualities schema to contain all of the assertions previously made in the credentials thus allowing for credentials to assert qualities by reference to an XML document based on this schema. Specifically, version 1.1 of this document adds the TPMSecurityAssertionsType and TBBSecurityAssertionsType complex types.

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:

```
version="version_number"
```

This document refers to version 1.10 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:

```
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_1#
```

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

schema location: http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1.xsd
attribute form default: **unqualified**
element form default: **qualified**
targetNamespace: http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

The following are the complex types defined within this specification.

Elements	Complex types
SecurityQualities	AdditionalInfoType
	CommonCriteriaType
	FipsLevelType
	Iso9000Type
	SecurityQualitiesType
	TBBSecurityAssertionsType
	TPMSecurityAssertionsType

3.1 Complex Types and Elements

3.1.1 complexType AdditionalInfoType

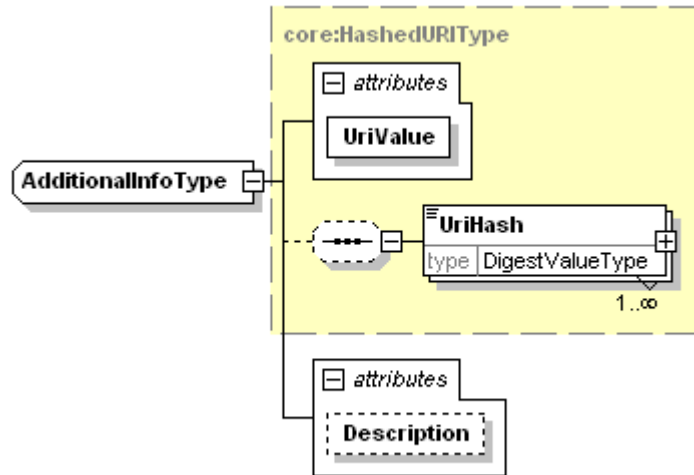
3.1.1.1 Description

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

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type extension of **core:HashedURIType**

properties base core:HashedURIType

children **UriHash**

used by elements [CommonCriteriaType/AdditionalInfo](#) [FipsLevelType/AdditionalInfo](#) [Iso9000Type/AdditionalInfo](#) [SecurityQualitiesType/AdditionalInfo](#) [CommonCriteriaType/CertificationBody](#) [CommonCriteriaType/ProfileLocation](#) [CommonCriteriaType/VerificationReport](#) [CommonCriteriaType/TargetLocation](#)

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

3.1.1.3 Attribute Detail

Attribute	Description
UriValue	Reference to a web document describing the security quality to be associated with the component.
Description	Textual description of the context of the security quality asserted in the document to aid the verifier's understand 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.

3.1.1.4 XML

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

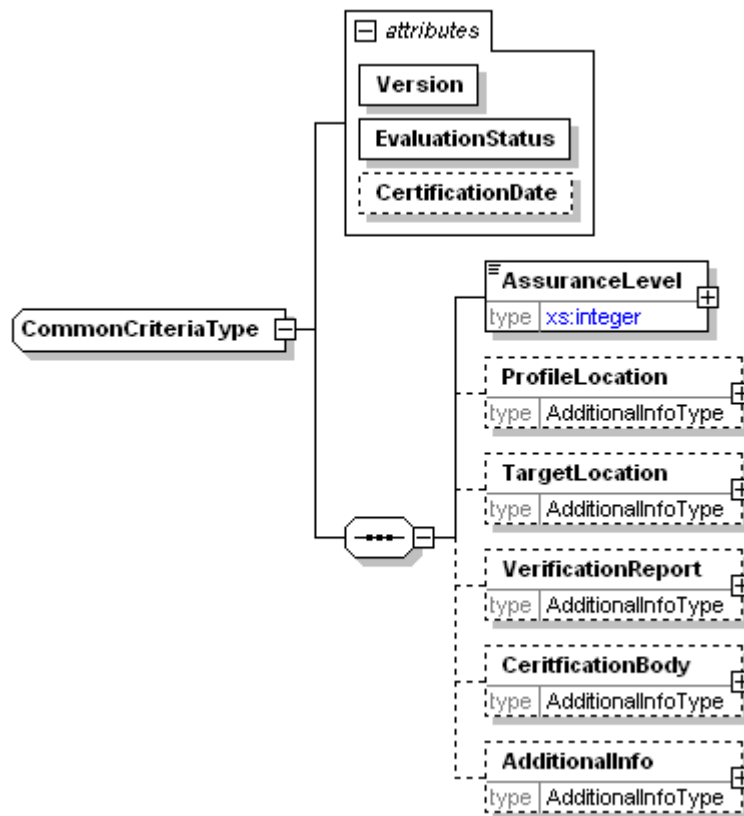
3.1.2 complexType CommonCriteriaType

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 contain 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

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

children [AssuranceLevel](#) [ProfileLocation](#) [TargetLocation](#) [VerificationReport](#) [CertificationBody](#) [AdditionalInfo](#)

used by element [SecurityQualitiesType/CommonCriteria](#)

attributes	Name	Type	Use	Default	Fixed
	Version	xs:normalizedString	required		
	EvaluationStatus	xs:NMTOKEN	required		
	CertificationDate	xs:date	optional		

3.1.2.3 Attribute Detail

Attribute	Description
-----------	-------------

Version	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 3.1 was recently released so this value describes which version of the process was applied to the product evaluation.
EvaluationStatus	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.
CertificationDate	Date when product received its common criteria evaluation. This attribute should only be included when Evaluation Status is EvaluationCompleted.

3.1.2.4 XML

```

source <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: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: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:complexType>

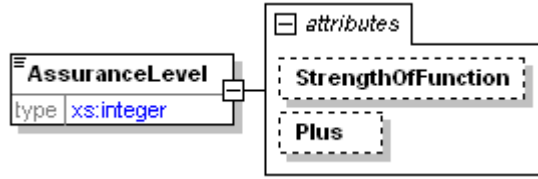
```

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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type extension of **xs:integer**

properties isRef 0
content complex

attributes	Name	Type	Use	Default	Fixed
	StrengthOfFunction	xs:NMTOKEN	optional		
	Plus	xs:boolean	optional		

3.1.3.2 Attribute Detail

Attribute	Description
StrengthOfFunction	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.
Plus	Additional indicator that the product went beyond the indicated assurance level.

3.1.3.3 XML

```

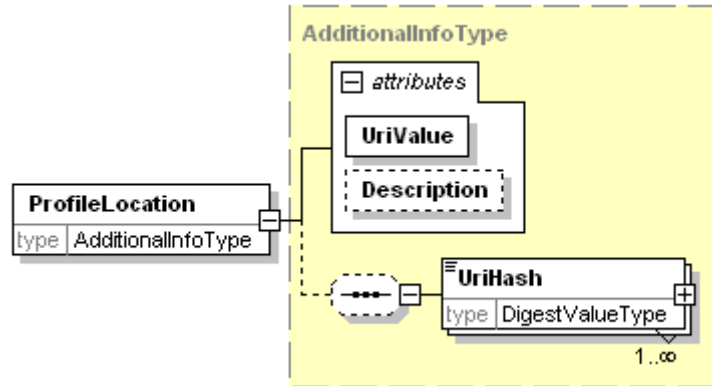
source <xs:element name="AssuranceLevel">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="xs:integer">
        <xs:attribute name="StrengthOfFunction" use="optional">
          <xs:simpleType>
            <xs:restriction base="xs:NMTOKEN">
              <xs:enumeration value="Basic"/>
              <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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children **UriHash**

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

3.1.4.2 Attribute Detail

Attribute	Description
UriValue	Location of the protection profile document expressed in URI format.
Description	Human readable description of the referenced protection profile document.

3.1.4.3 XML

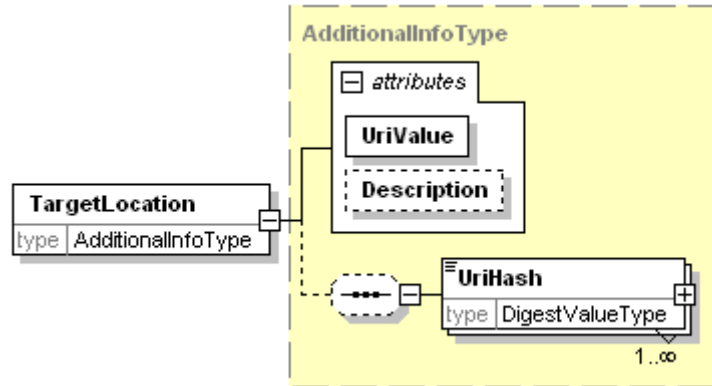
source `<xs:element name="ProfileLocation" type="AdditionalInfoType" minOccurs="0"/>`

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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children **UriHash**

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

3.1.5.2 Attribute Detail

Attribute	Description
UriValue	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.
Description	Human readable description of the security target document being referenced.

3.1.5.3 XML

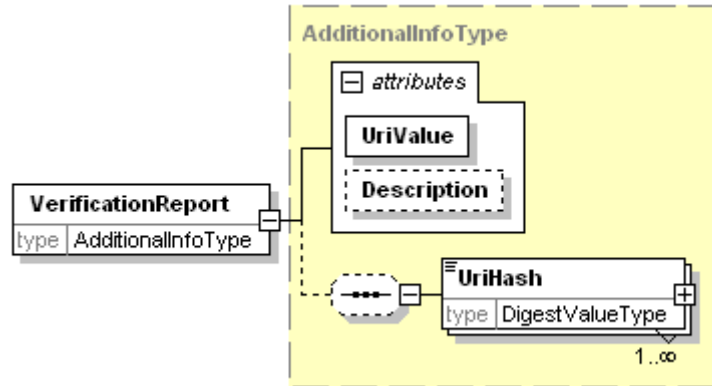
source `<xs:element name="TargetLocation" type="AdditionalInfoType" minOccurs="0"/>`

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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children **UriHash**

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

3.1.6.2 Attribute Detail

Attribute	Description
UriValue	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.
Description	Human readable Information about the verification report referenced by UriValue.

3.1.6.3 XML

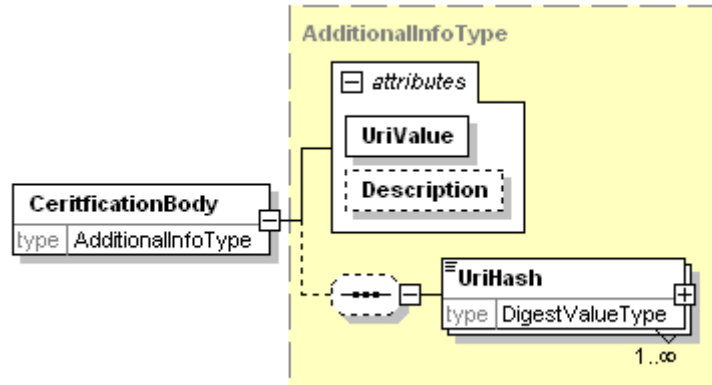
source `<xs:element name="VerificationReport" type="AdditionalInfoType" minOccurs="0"/>`

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_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children UriHash

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

3.1.7.2 Attribute Detail

Attribute	Description
UriValue	URI formatted location of a web page or document which describes the certifying body which performed the evaluation of the component.
Description	Human readable description of the document referenced by UriValue.

3.1.7.3 XML

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

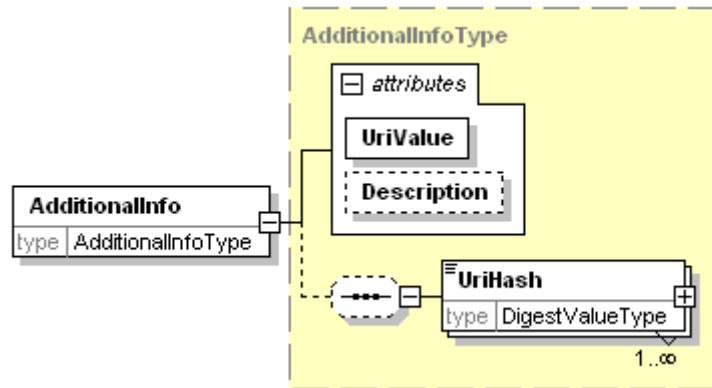
3.1.8 element CommonCriteriaType/AdditionalInfo

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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children UriHash

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

3.1.8.2 Attribute Detail

Attribute	Description
UriValue	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.
Description	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.

3.1.8.3 XML

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

3.1.9 complexType FipsLevelType

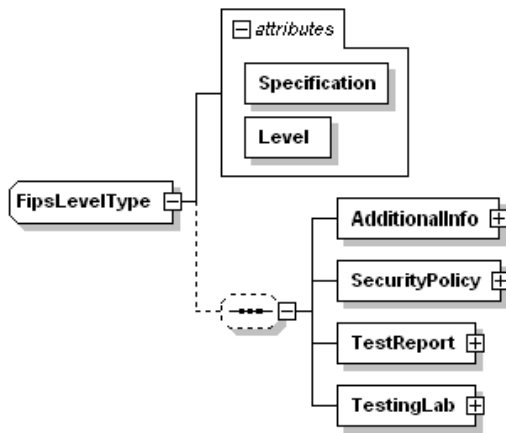
3.1.9.1 Description

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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

children [AdditionalInfo](#) [SecurityPolicy](#) [TestReport](#) [TestingLab](#)

used by element [SecurityQualitiesType/FipsLevel](#)

attributes	Name	Type	Use	Default	Fixed
	Specification	xs:normalizedString	required		
	Level	xs:integer	required		

3.1.9.2 Attribute Detail

Attribute	Description
Specification	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"
Level	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.

3.1.9.3 XML

```

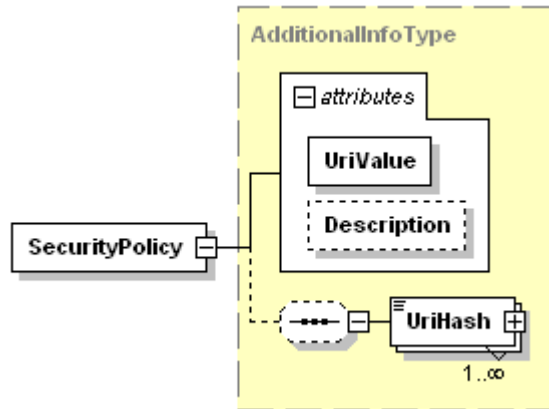
source <xs:complexType name="FipsLevelType">
  <xs:sequence minOccurs="0">
    <xs:element name="AdditionalInfo" type="AdditionalInfoType"/>
    <xs:element name="SecurityPolicy" type="AdditionalInfoType"/>
    <xs:element name="TestReport" type="AdditionalInfoType"/>
    <xs:element name="TestingLab" 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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children **UriHash**

attributes	Name	Type	Use	Default	Fixed	Annotation
	UriValue	xs:anyURI	required			
	Description	xs:string	optional			

3.1.10.2 Attribute Detail

Attribute	Description
UriValue	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.
Description	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.

3.1.10.3 XML

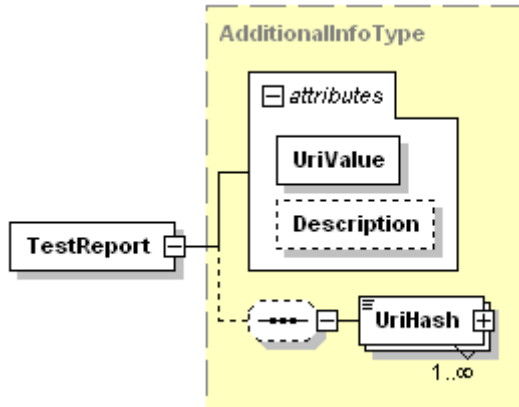
source `<xs:element name="SecurityPolicy" type="AdditionalInfoType"/>`

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



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children UriHash

attributes	Name	Type	Use	Default	Fixed	Annotation
	UriValue	xs:anyURI	required			
	Description	xs:string	optional			

3.1.11.2 Attribute Detail

Attribute	Description
UriValue	URI formatted reference to the test report associated with the associated component.
Description	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.

3.1.11.3 XML

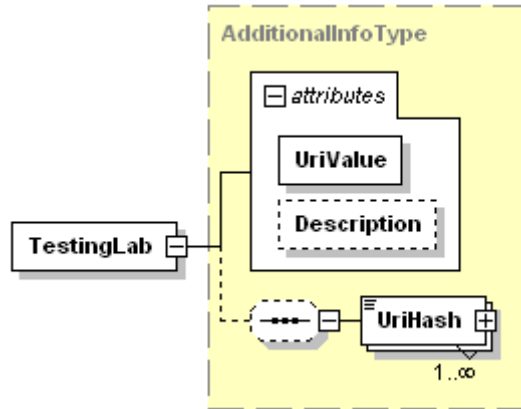
source `<xs:element name="TestReport" type="AdditionalInfoType"/>`

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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children **UriHash**

attributes	Name	Type	Use	Default	Fixed	Annotation
	UriValue	xs:anyURI	required			
	Description	xs:string	optional			

3.1.12.2 Attribute Detail

Attribute	Description
UriValue	URI formatted reference to an available document describing the laboratory that performed the validation testing on the component.
Description	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.

3.1.12.3 XML

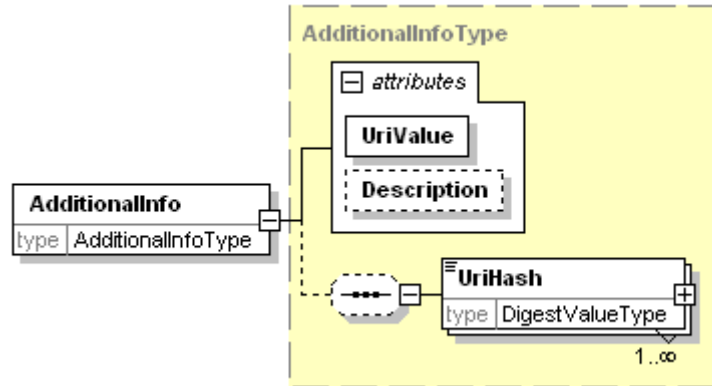
source `<xs:element name="TestingLab" type="AdditionalInfoType"/>`

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.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [AdditionalInfoType](#)

properties isRef 0
content complex

children **UriHash**

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

3.1.13.2 Attribute Detail

Attribute	Description
UriValue	URI formatted reference to an available document describing some aspect of the FIPS evaluation process of the component.
Description	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.

3.1.13.3 XML

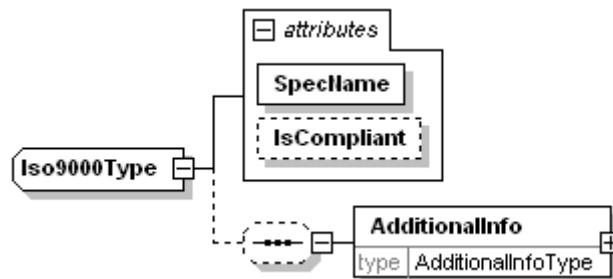
source `<xs:element name="AdditionalInfo" type="AdditionalInfoType"/>`

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.

diagram



namespace	http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#				
children	AdditionalInfo				
used by	element	SecurityQualitiesType/Iso9000			
attributes	Name	Type	Use	Default	Fixed
	SpecName IsCompliant	xs:NMTOKEN xs:boolean	required optional		

3.1.14.2 Attribute Detail

Attribute	Description
SpecName	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 "ISO 9000:2000" if this version of the ISO 9000 specification was used.
IsCompliant	Boolean result of whether the environment used to design and build the component met the associated ISO 9000 criteria.

3.1.14.3 XML

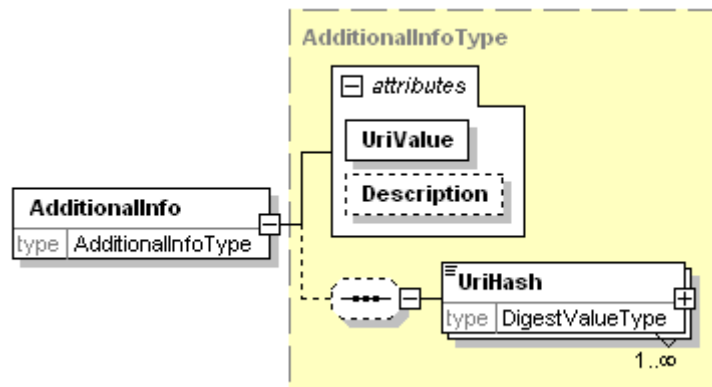
```
source <xs:complexType name="Iso9000Type">
  <xs:sequence minOccurs="0">
    <xs:element name="AdditionalInfo" type="AdditionalInfoType"/>
  </xs:sequence>
  <xs:attribute name="SpecName" type="xs:NMTOKEN" use="required"/>
  <xs:attribute name="IsCompliant" type="xs:boolean"/>
</xs:complexType>
```

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.

diagram



namespace	http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#		
type	AdditionalInfoType		
properties	isRef	0	
	content	complex	
children	UriHash		

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

3.1.15.2 Attribute Detail

Attribute	Description
UriValue	URI formatted reference to a document describing more information about the application of the ISO 9000 evaluation processes or results associated with the component.
Description	Human readable description of the referenced document.

3.1.15.3 XML

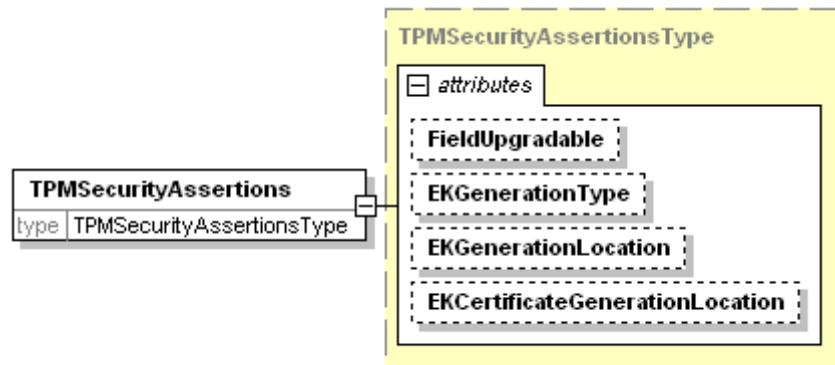
source `<xs:element name="AdditionalInfo" type="AdditionalInfoType"/>`

3.1.16 complexType TPMSecurityAssertionsType

3.1.16.1 Description

This complex type describes the security assertions typically made about the TPM within the TCG Credentials specification version 1.0. These assertions describe properties of how the EK was created and whether it can be upgraded in the field.

diagram



namespace `http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#`

type [TPMSecurityAssertionsType](#)

properties isRef 0
content complex

attributes	Name	Type	Use	Default
	FieldUpgradable	xs:boolean	Optional	
	EKGenerationType	xs:NMTOKEN	Optional	
	EKGenerationLocation	xs:NMTOKEN	Optional	
	EKCertificateGenerationLocation	xs:NMTOKEN	Optional	

3.1.16.2 Attribute Detail

Attribute	Description
FieldUpgradable	Indicates whether the TPM is capable of being field upgraded.

EKGenerationType	<p>Describes whether the EK (key pair) was generated inside the TPM (INTERNAL) or externally and injected (INJECTED) into the TPM. This type also indicates whether the EK can be revoked should it be potentially exposed. Referring to the XML for the enumeration values, those values with REVOCABLE in their name also represent that the EK is revocable (INJECTEDREVOCABLE means the EK was generated externally and injected into the TPM and the EK can be revoked if necessary.)</p> <p>If the EKGenerationLocation is not TPMMANUFACTURER, then EKGenerationType SHOULD NOT be INJECTED or INJECTEDREVOCABLE as the TPM normally wouldn't offer a capability to inject this late in the supply chain.</p>
EKGenerationLocation	<p>Asserts the party within the supply chain which created the EK. The specific parties enumerated include: the TPM manufacturer, Platform Manufacturer, and Owner (possibly IT department or other parties late in the supply chain) who might be identified by their issuer name in the EK Certificate. Generally an EK created earlier in the supply chain is considered more trustworthy (for instance the TPM manufacturer is most familiar with the part and likely controls access to it during manufacturing) so a verifier might be interested in this information.</p>
EKCertificateGenerationLocation	<p>This is analogous to the EKGenerationLocation however asserts when in the supply chain the EK Certificate was issued. The enumeration values are the same as above except the TRUSTED3RDPARTY is added to recognize when a 3rd party (like a Privacy CA) is used by a deployment to issue the EK Certificate. The EK Certificate can be issued at a time much later in the supply chain than when the EK key pair are created and thus be done by a different party (e.g. IT) or might not be issued at all.</p>

3.1.16.3 XML

```

source <xs:complexType name="TPMSecurityAssertionsType">
  <xs:attribute name="FieldUpgradable" type="xs:boolean"/>
  <xs:attribute name="EKGenerationType">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
        <xs:enumeration value="INJECTEDREVOCABLE"/>
        <xs:enumeration value="INTERNALREVOCABLE"/>
        <xs:enumeration value="INJECTED"/>
        <xs:enumeration value="INTERNAL"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="EKGenerationLocation">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
        <xs:enumeration value="TPMMANUFACTURER"/>
        <xs:enumeration value="PLATFORMMANUFACTURER"/>
        <xs:enumeration value="OWNER"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="EKCertificateGenerationLocation">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
        <xs:enumeration value="TPMMANUFACTURER"/>
        <xs:enumeration value="PLATFORMMANUFACTURER"/>
        <xs:enumeration value="OWNER"/>
        <xs:enumeration value="TRUSTED3RDPARTY"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>

```

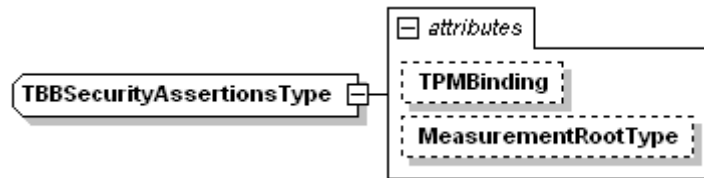
</xs:complexType>

3.1.17 complexType TBBSecurityAssertionsType

3.1.17.1 Description

This complex type describes the security assertions typically made about the TBB (includes the platform chipset) within the TCG Credentials specification version 1.0. These assertions describe the security capabilities of the platform. For instance, an OEM might assert that the platform is capable of dynamically invoking the RTM.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

type [TBBSecurityAssertionsType](#)

properties isRef 0
content complex

attributes	Name	Type	Use	Default	Fixed
	TPMBinding	xs:NMTOKEN	Optional		
	MeasurementRootType	xs:unsignedInt	Optional		

3.1.17.2 Attribute Detail

Attribute	Description
TPMBinding	<p>This enumeration indicates how the TPM is associated (or bound) to the platform.</p> <p>Frequently the TPM is physically attached to the platform (e.g. soldered) or is integrated within a platform component (e.g. gates in a CPU) which is considered a 1 – physical.</p> <p>The TPM may be logically bound to the platform possibly using cryptographic techniques to prove the linkage. If this approach is used to associate the TPM to the TBB, this is considered a 2 – logical.</p> <p>Another type of TPM binding is virtual where the TPM might be implemented in software and is associated with the other trusted roots via virtualization techniques. This is considered a 3 – virtualized.</p> <p>If this document creator is unsure of the binding technique used, this attribute should not be asserted.</p>
MeasurementRootType	<p>Bitmap indicating properties of the Root of Trust for Measurement (RTM) and how it is instantiated on this platform. This attribute is a bitmap recognizing that a single platform may support multiple types of measurement roots. The currently defined bit definitions (from the least significant bit) are: 1 – static, 2 – dynamic, 3 – nonhost, bits 4-32 are reserved for future use.</p> <p>The static and dynamic bits refer to whether the CRTM can be invoked at the start of the boot sequence (static) and/or whether it may be started later after the operating system has starting running (dynamic.)</p>

The nonhost bit indicates the RTM executes within a component on the system other than the main CPU. For example, nonhost might be a service processor as described by the PC Client specification.

If the document creator has knowledge that the platform does not have a measurement root, it SHOULD set this value to 0 to indicate none present. If the creator is unaware of what type of root is present in the platform, it SHOULD NOT include this attribute.

The reserved bits SHOULD be set to 0 and MUST be ignored by verifiers.

3.1.17.3 XML

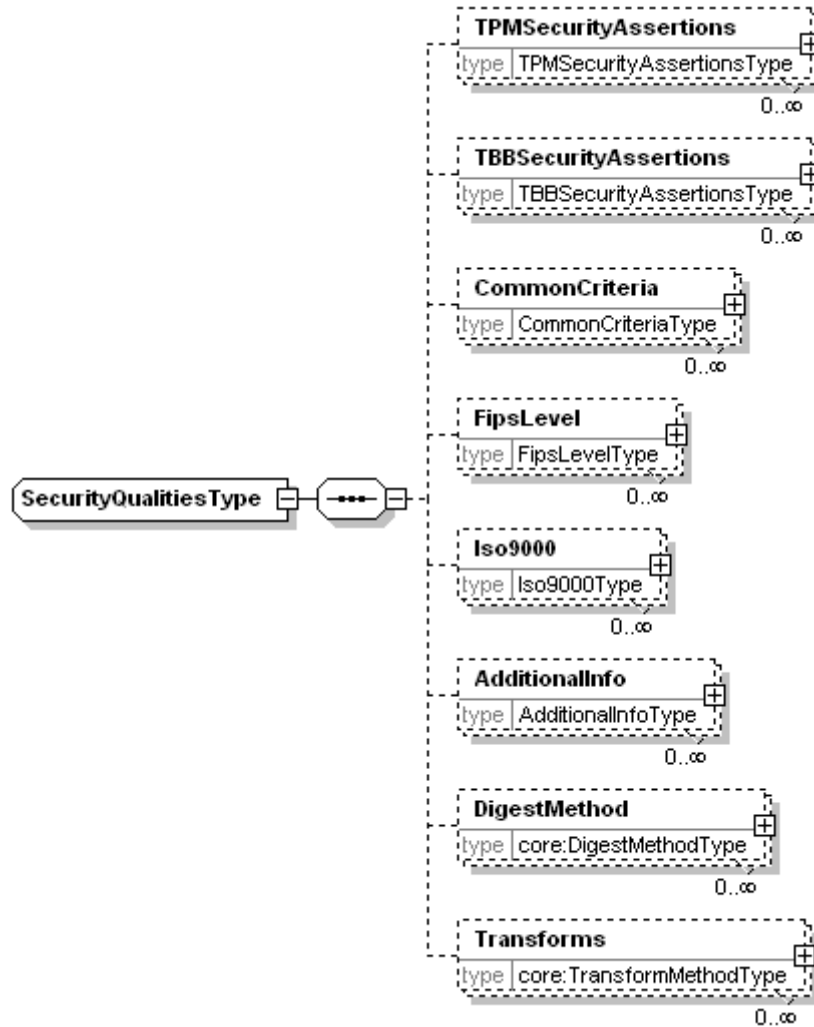
```
source <xs:complexType name="TBBSecurityAssertionsType">
  <xs:attribute name="TPMBinding">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
        <xs:enumeration value="PHYSICAL"/>
        <xs:enumeration value="LOGICAL"/>
        <xs:enumeration value="VIRTUAL"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="MeasurementRootType">
    <xs:simpleType>
      <xs:restriction base="xs:unsignedInt">
        <xs:enumeration value="1"/>
        <xs:enumeration value="2"/>
        <xs:enumeration value="4"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:complexType>
```

3.1.18 complexType SecurityQualitiesType

3.1.18.1 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 and assertions about un-measurable properties of the TPM and TBB.

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Security_Qualities_v1_1#

children [TPMSecurityAssertions](#) [TBBSecurityAssertions](#) [CommonCriteria](#) [FipsLevel](#) [Iso9000](#) [AdditionalInfo](#) [DigestMethod](#) [Transforms](#)

used by element [SecurityQualities](#)

3.1.18.2 Attribute Detail

Attribute	Description
None	

3.1.18.3 XML

```

source <xs:complexType name="SecurityQualitiesType">
  <xs:sequence>
    <xs:element name="TPMSecurityAssertions" type="TPMSecurityAssertionsType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="TBBSecurityAssertions" type="TBBSecurityAssertionsType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="CommonCriteria" type="CommonCriteriaType" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="FipsLevel" type="FipsLevelType" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
  
```

```
<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

- [1] Trusted Computing Group, TCG IWG Reference Manifest Schema, Specification Version 1.0, Revision 0.8, November 2006, https://www.trustedcomputinggroup.org/specs/IWG/Reference_Manifest_Schema_Specification_v1.0.pdf
- [2] Trusted Computing Group, TCG IWG Core Integrity Schema, Specification Version 1.0, Revision 1.0, November 2006, https://www.trustedcomputinggroup.org/specs/IWG/CoreIntegrity_Schema_Specification_v1.0.1.pdf
- [3] W3C, XML Schema, W3C Consortium, October 2004.
- [4] National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 140-1, January, 1994. <http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf>
- [5] National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication 140-2, May, 2001. <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- [6] Common Criteria, Common Criteria evaluation process information portal, <http://www.commoncriteriaportal.org/public/consumer/>
- [7] Common Criteria, Common Criteria for Information Security Technology Evaluation, August 2005. <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2>
- [8] International Organization for Standardization, ISO 9000 / ISO 14000 Portal. <http://www.iso.org/iso/en/iso9000-14000/index.html>
- [9] Trusted Computing Group, TCG Credentials Profile, Specification Version 1.0, January 2006, https://www.trustedcomputinggroup.org/specs/IWG/Credential_Profiles_V1_R0.981-2.pdf
- [10] Security Qualities Schema Specification, Version 1.0, Rev. 1.0 https://www.trustedcomputinggroup.org/specs/IWG/SecurityQualities_Schema_Specification_v1.0.pdf