TCG Infrastructure Working Group Integrity Report Schema

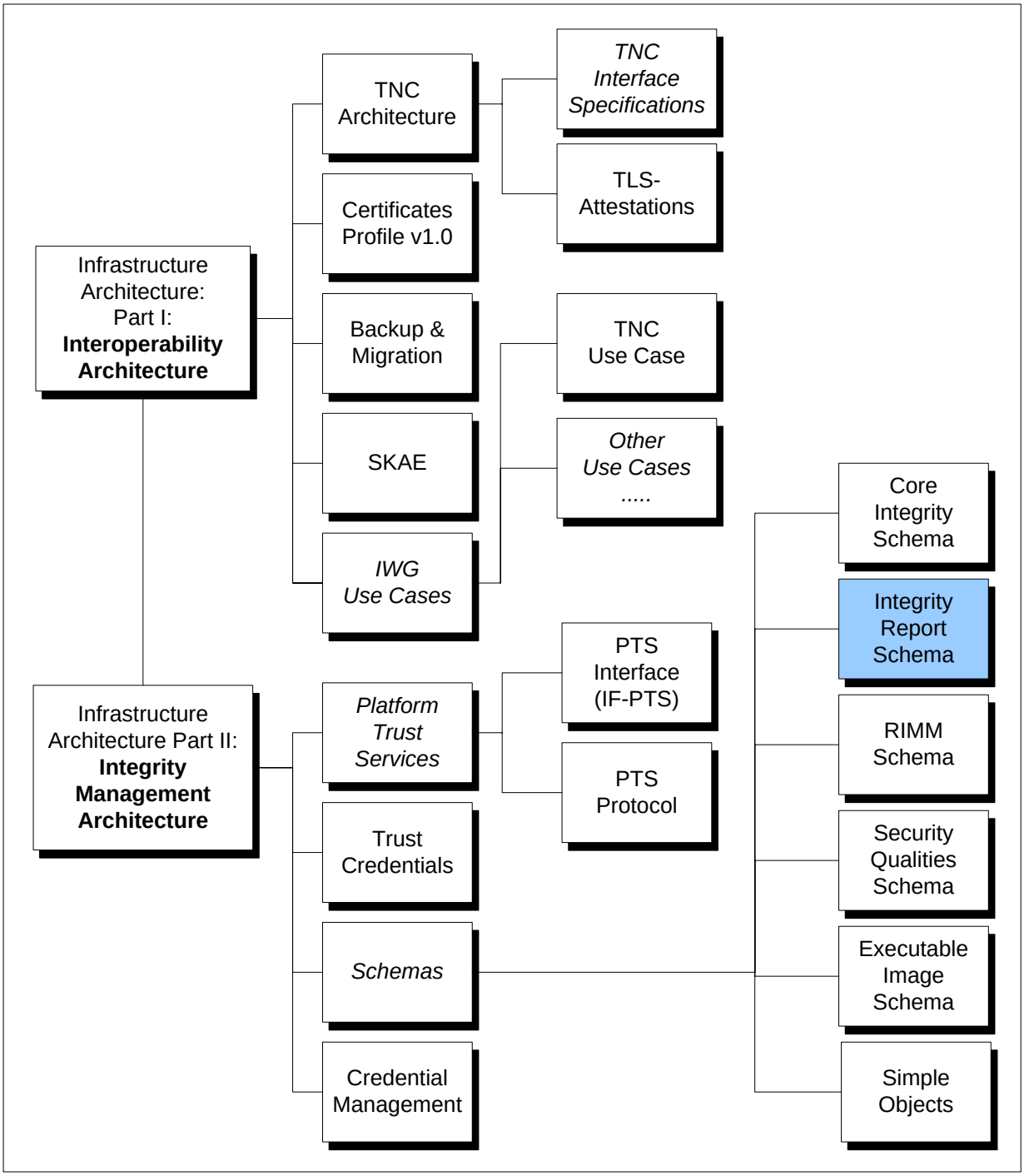
Specification Version 2.0
Revision 5
August 24, 2011
PUBLISHED

Contacts:
admin@trustedcomputinggroup.org

TCG Published

TCG

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:

Diana Arroyo	IBM
David Bleckman	Signacert
Mike Boyle	US Government
Rene Bourquin	General Dynamics C4 Systems
Carlin Covey	Freescale Semiconductor
Malcolm Duncan	CESG
Markus Gueller	Infineon
Thomas Hardjono	MIT
Wyllys Ingersoll (editor, IWG Co-chair)	Oracle
Greg Kazmierczak	Wave Systems
Carolin Latze	89grad GmbH
Kazuaki Nimura	Fujitsu Limited
Jeff Nisewanger	SUN
Gilles Peskine	Gemalto SA
Mark Redman	Freescale Semiconductor
Paul Sangster (IWG Co-chair)	Symantec
Gloria Serrao	US Government
Ned Smith	Intel
Adrian Stanger	US Government
Lee Terrell	IBM
Len Veil	Wave Systems
Lee Wilson	IBM

Table of Contents

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 integrity report metadata XML schema defines the structure with which integrity information is communicated between entities.

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

The purpose of this document is to provide a detailed description of the TCG Infrastructure Working Group's integrity report XML schema, hereafter referred to as the *report schema*. The report schema is derived from the Core Integrity Schema [1].

The report schema allows instantiation of interoperable integrity reports and snapshots including data structures provided by a 1.1 or 1.2 Level TPM. Integrity reports based on the report schema are used to detail run-time measurements and assertions of the components of a system to a verifier. One use of integrity reports and structures is in the Trusted Network Connect (TNC) use models [7] whereby a Platform Trust Service (PTS) [8] creates integrity reports and snapshots to be sent by IMCs to their corresponding IMVs for verification of acceptable platform state prior to network access.

2.1 Schema Version

The report 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 2.0 of the report schema. Consumers of an integrity report should check the schema version prior to parsing the remainder of the integrity report to determine if the version is supported.

2.2 Schema Namespace

The report 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/2_0/integrity_report#
```

2.3 Dependent Schema Definitions

2.3.1 W3C XML Schema Syntax

The report schema relies upon data structures defined by the World Wide Web Consortium's (W3C) XML-Schema syntax. Consequently, the report schema imports the W3C's XML schema with the following namespace:

```
http://www.w3.org/2001/XMLSchema
```

The report schema associates the abovementioned schema with the "xs" namespace prefix.

2.3.2 W3C XML-Signature Syntax

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

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

The report schema associates the abovementioned schema with the "ds" namespace prefix.

2.3.3 TCG Core Integrity Schema Syntax

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

```
      http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/core_integrit
y#
```

The report schema associates the abovementioned schema with the “core” namespace prefix.

2.3.4 Schema Diagram 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.

2.3.5 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 Integrity Report Schema

schema location: http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report
attribute form default: Unqualified
element form default: Qualified
targetNamespace: http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

3.1 COMPLEX TYPES

The following complex types are specified in this document:

Complex types
CapVersionInfoType
CompositeHashType
DigestValueType
old-SnapshotRefType
PcrCompositeType
PcrInfoShortType
PcrSelectionType
Quote2Type
QuoteDataType
QuoteInfo2Type
QuoteInfoType
QuoteSignatureType
QuoteType
ReportType
SnapshotType
TpmDigestValueRestrictionType
TpmDigestValueType

Elements which are derived from these complex types are defined in section 3.2.

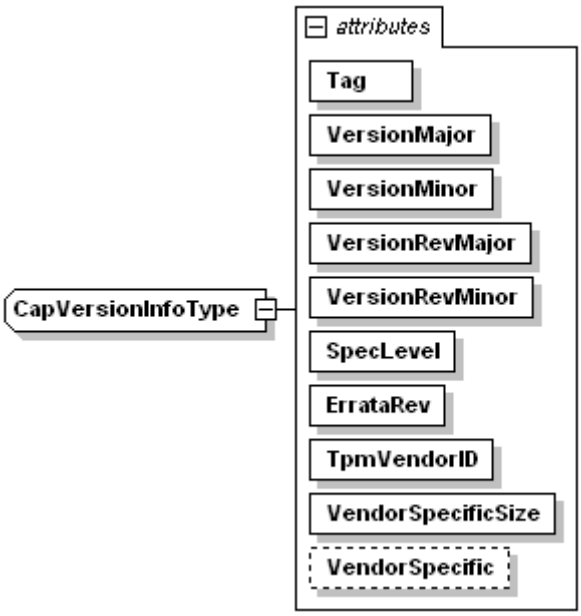
3.1.1 complexType CapVersionInfoType

3.1.1.1 Description

The CapVersionInfoType complex type represents in XML the information optionally returned by a 1.2 TPM from a call to the optional TPM command Quote2 or by a call to the TPM command GetCapability for CAP_VERSION_INFO – it is the identical information independent of the two origins. Quote2 is not supported in a 1.1b TPM, but is an optional command in a 1.2 TPM – however it is a required command in a PC Client platform. CapVersionInfoType represents in XML the TPM version and vendor information. Refer to [2] for definition of TPM structures.

3.1.1.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

used by elements QuoteType/TpmInfo/CapVersionInfo Quote2Type/CapVersionInfo

attributes

Name	Type	Use	Default	Fixed
Tag	xs:unsignedShort	required		
VersionMajor	xs:unsignedByte	required		
VersionMinor	xs:unsignedByte	required		
VersionRevMajor	xs:unsignedByte	required		
VersionRevMinor	xs:unsignedByte	required		
SpecLevel	xs:unsignedShort	required		
ErrataRev	xs:unsignedByte	required		
TpmVendorID	xs:normalizedString	required		
VendorSpecificSize	xs:unsignedShort	required		
VendorSpecific	xs:base64Binary	optional		

3.1.1.3 Attribute Detail

Attribute	Description
Tag	The TPM specifications state this is TPM_TAG_CAP_VERSION_INFO and has a value of 0x0030.
VersionMajor	This is the TPM major version number. The TPM specifications state this attribute has a value of 0x0100. This number corresponds to the “1” in a 1.2 TPM.
VersionMinor	This is the TPM minor version number. The TPM specifications state this attribute is 0x0100 (for TPM 1.1b) or 0x0200 (for TPM 1.2).
VersionRevMajor	The TPM specifications state this attribute is the value of the TPM_PERMANENT_DATA -> revMajor. I.e. this is a vendor specific major version number.
VersionRevMinor	The TPM specifications state this attribute is the value of the TPM_PERMANENT_DATA -> revMinor. I.e. this is a vendor specific minor version number.
SpecLevel	SpecLevel is defined in the TCG document “Specification Naming and Numbering”. The SpecLevel corresponds to a TPM specification version release of a particular Major.Minor version. The number indicates the level of ordinals supported. A new Spec Level is assigned for each version of TPM specification that adds or deletes ordinals.
ErrataRev	A number indicating the errata version of the specification and indicates changes to a TPM specification that does not include new or deleted ordinals. For older TPMs (1.1 or early 1.2 TPMs), the errata revision was a “letter”. E.g.,

	1.1”a” or 1.1”b”; however the currently specification naming and numbering guidelines only support ErrataRev numbers.
TpmVendorID	TpmVendorID is a value unique to each vendor. The TPM specifications state this attribute is a 4-byte value that is usually the vendor’s stock ticker value in capitalized characters. If the string is less than 4 bytes long, it should be padded with trailing NULLs prior to use.
VendorSpecificSize	TPM vendor defined area to the TPM vendor’s needs.
VendorSpecific	The vendor specific area allows the TPM vendor to provide support for vendor options.

3.1.1.4 XML

source
```
<xs:complexType name="CapVersionInfoType">
  <xs:attribute name="Tag" type="xs:unsignedShort" use="required"/>
  <xs:attribute name="VersionMajor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="VersionMinor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="VersionRevMajor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="VersionRevMinor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="SpecLevel" type="xs:unsignedShort" use="required"/>
  <xs:attribute name="ErrataRev" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="TpmVendorID" type="xs:normalizedString" use="required">
  <xs:attribute name="VendorSpecificSize" type="xs:unsignedShort" use="required"/>
  <xs:attribute name="VendorSpecific" type="xs:base64Binary" use="optional"/>
</xs:complexType>
```

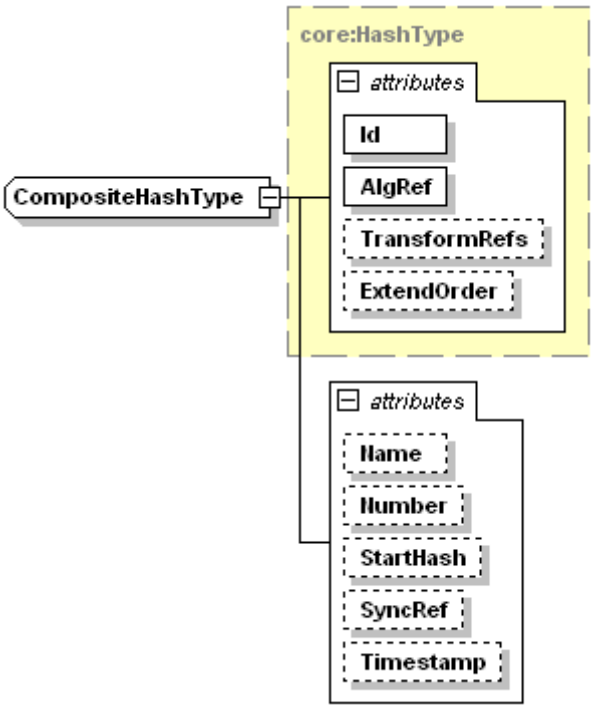
3.1.2 complexType CompositeHashType

3.1.2.1 Description

The CompositeHashType complex type is an extension of the core:HashType complex type defined in [2]. This is the end digest value in a snapshot of the values referenced by the ExtendOrder attribute. CompositeHashType extends core:HashType by adding the following optional attributes: Name, Number, StartHash, SyncRef, and TimeStamp. CompositeHashType complex types should be used for non-PCR digests, but may themselves be extended into a PCR. The digest is a hash across the measurements in a snapshot so that changes to any of the measurements can be detected. A verifier MUST use the ExtendOrder attribute to traverse the tree to correctly recreate this value.

3.1.2.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type extension of **core:HashType**

properties base core:HashType

used by element **SnapshotType/CompositeHash**

attributes

Name	Type	Use	Default	Fixed
Id	xs:ID	required		
AlgRef	xs:IDREF	required		
TransformRefs	xs:IDREFS	optional		
ExtendOrder	xs:IDREFS	optional		
Name	xs:normalizedString	optional		
Number	xs:integer	optional		
StartHash	ds:DigestValueType	optional		
SyncRef	xs:IDREF	optional		
Timestamp	xs:dateTime	optional		

3.1.2.3 Attribute Detail

Attribute	Description
Id	Integrity Report document unique Record instance identifier – uniqueness is only guaranteed within the XML document. Id can be used in other parts of the XML document and by external systems to reference the CompositeHash instance in an integrity report.
AlgRef	AlgRef refers to a hash algorithm as defined by DigestMethodType
TransformRefs	Refers to transformation functions, used to modify the data prior to performing the digest, idefined by TransformMethod elements of type TransformMethodType
ExtendOrder	ExtendOrder contains an ordered list of xs:IDREF values. Values at the beginning of the list occur before values at the end. Therefore, the first entry in the list would be the first value extended, the last entry would be the last value extended.
Name	A string name assigned to the CompositeHash. The string name may be useful to a verifier when referencing the snapshot digest value and an xs:Id does not provide

	enough descriptive detail.
Number	A number assigned to the CompositeHash
StartHash	The initial value of the CompositeHash prior to extending values. If this attribute is not populated, a null initial value is assumed.
SyncRef	SyncRef is an xs:IDREF reference to the sync snapshot if the CompositeHash has been included in a sync snapshot. A sync snapshot is the snapshot that corresponds to a TPM PCR. Regular snapshots MAY be included in the PCR digest by extending the CompositeHash value into the TPM PCR (i.e. by calling the SyncSnapshot command in [8]). SyncRef allows the verifier to easily find the sync snapshot, especially if the integrity report contains more than 1 sync snapshot.
Timestamp	Timestamp is a date and time reference when the CompositeHash was calculated.

3.1.2.4 XML

source

```
<xs:complexType name="CompositeHashType">
  <xs:simpleContent>
    <xs:extension base="core:HashType">
      <xs:attribute name="Name" type="xs:normalizedString"/>
      <xs:attribute name="Number" type="xs:integer"/>
      <xs:attribute name="StartHash" type="ds:DigestValueType"/>
      <xs:attribute name="SyncRef" type="xs:IDREF"/>
      <xs:attribute name="Timestamp" type="xs:dateTime"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

3.1.3 complexType PcrCompositeType

3.1.3.1 Description

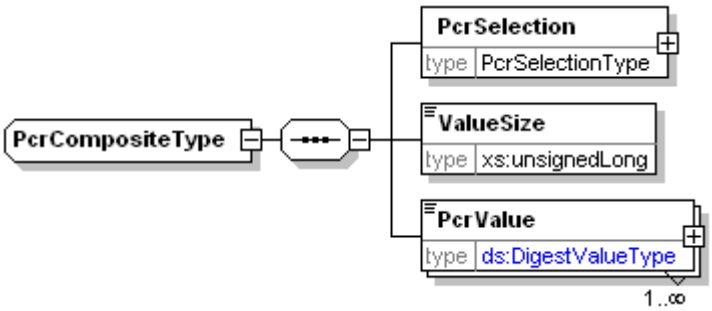
The PcrCompositeType complex type is used to aggregate multiple PCR values in a single structure and represents, in XML, the TPM's TPM_PCR_COMPOSITE structure returned from a call to Quote TPM PCRs. Refer to [2] for definition of TPM structures.

Elements of PcrCompositeType include:

- PcrSelection – identifies which TPM PCRs are quoted
- ValueSize – the length in bytes of the array of PcrValue complex types
- PcrValue - The array of PcrValue structures. Each PcrValue contains a PCR number attribute to correspond to a PCR identified in PcrSelection. The PCR value itself is not included, but may be found in the Quote structure. In addition, PcrValue contains an optional reference to the snapshot that provides the corresponding details including PCR value.

3.1.3.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **PcrSelection** **ValueSize** **PcrValue**

used by elements **QuoteType/PcrComposite** **PcrInfoShortType/PcrComposite**

3.1.3.3 XML

source

```
<xs:complexType name="PcrCompositeType">
  <xs:sequence>
    <xs:element name="PcrSelection" type="PcrSelectionType"/>
    <xs:element name="ValueSize" type="xs:unsignedLong"/>
    <xs:element name="PcrValue" maxOccurs="unbounded">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="ds:DigestValueType">
            <xs:attribute name="SnapshotRef" type="xs:IDREF" use="optional"/>
            <xs:attribute name="PcrNumber" type="xs:unsignedLong" use="required"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

3.1.4 complexType PcrInfoShortType

3.1.4.1 Description

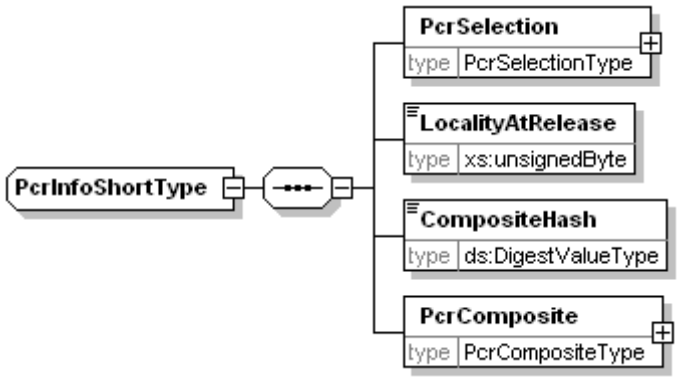
The PcrInfoShortType complex type is an XML representation of the TPM's TPM_PCR_INFO_SHORT structure. PcrComposite is not part of the TPM PCR_INFO_SHORT structure, however CompositeHash is a hash of PcrComposite, thus PcrComposite is included to provide the data necessary to compute and validate CompositeHash. Refer to [2] for definition of TPM structures.

Elements include:

- PcrSelection – PcrSelection defines which TPM PCRs are used in the TPM Quote.
- LocalityAtRelease - TPM_PCR_INFO_SHORT includes locality information to provide the requestor a more complete view of the current platform configuration
- CompositeHash – A hash of PcrComposite
- PcrComposite – A TPM_PCR_COMPOSITE structure containing the actual values of the PCRs quoted.

3.1.4.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **PcrSelection** **LocalityAtRelease** **CompositeHash** **PcrComposite**

used by element **QuoteInfo2Type/PcrInfoShort**

3.1.4.3 XML

source
```
<xs:complexType name="PcrInfoShortType">
  <xs:sequence>
    <xs:element name="PcrSelection" type="PcrSelectionType"/>
    <xs:element name="LocalityAtRelease" type="xs:unsignedByte"/>
    <xs:element name="CompositeHash" type="ds:DigestValueType"/>
    <xs:element name="PcrComposite" type="PcrCompositeType"/>
  </xs:sequence>
</xs:complexType>
```

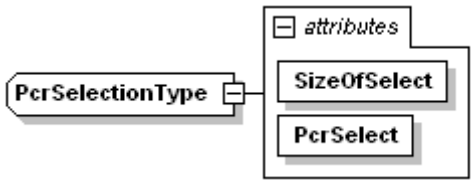
3.1.5 complexType PcrSelectionType

3.1.5.1 Description

The PcrSelectionType complex type is used to render the TPM's TPM_PCR_SELECTION structure. PcrSelectionType contents specify which PCRs are Quoted in an Integrity Report. Refer to [2] for definition of TPM structures.

3.1.5.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

used by elements **PcrCompositeType/PcrSelection** **PcrInfoShortType/PcrSelection**

attributes

Name	Type	Use	Default	Fixed
SizeOfSelect	xs:unsignedShort	required		
PcrSelect	xs:base64Binary	required		

3.1.5.3 Attribute Detail

Attribute	Description
SizeOfSelect	The size in bytes of the PcrSelect structure
PcrSelect	PcrSelect is a contiguous bit map that shows which PCRs are selected. Each byte represents 8 PCRs. Byte 0 indicates PCRs 0-7, byte 1 8-15 and so on. For each byte, the individual bits represent a corresponding PCR.

3.1.5.4 XML

source
```
<xs:complexType name="PcrSelectionType">
  <xs:attribute name="SizeOfSelect" type="xs:unsignedShort" use="required"/>
  <xs:attribute name="PcrSelect" type="xs:base64Binary" use="required"/>
</xs:complexType>
```

3.1.6 complexType Quote2Type

3.1.6.1 Description

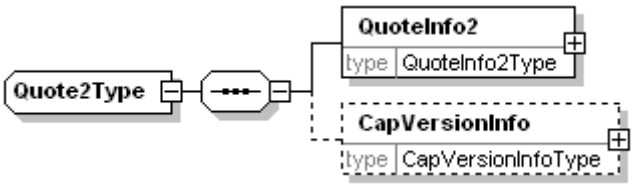
The Quote2Type complex type contains data returned from a call to the 1.2 TPM command Quote2 (not supported in a 1.1b TPM) except for the actual Quote2 signature (this is in the TpmSignature element), plus any other data necessary to compute and validate the Quote2 signature. Refer to [2] for definition of TPM structures.

Elements included are:

- QuoteInfo2 – The Quote2 data returned from the TPM plus any other data necessary to compute and validate the Quote2 signature. The Quote2 signature is not included here.
- CapVersionInfo – TPM Version information may optionally be returned by Quote2 or by a call to GetCapability; the data is identical independent of the method used to collect it. This information may be useful if the Quote2 data contains any vendor-specific interpretations.

3.1.6.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **QuoteInfo2** **CapVersionInfo**

used by element **QuoteDataType/Quote2**

3.1.6.3 XML

source

```
<xs:complexType name="Quote2Type">
  <xs:sequence>
    <xs:element name="QuoteInfo2" type="QuoteInfo2Type"/>
    <xs:element name="CapVersionInfo" type="CapVersionInfoType" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
```

3.1.7 complexType QuoteDataType

3.1.7.1 Description

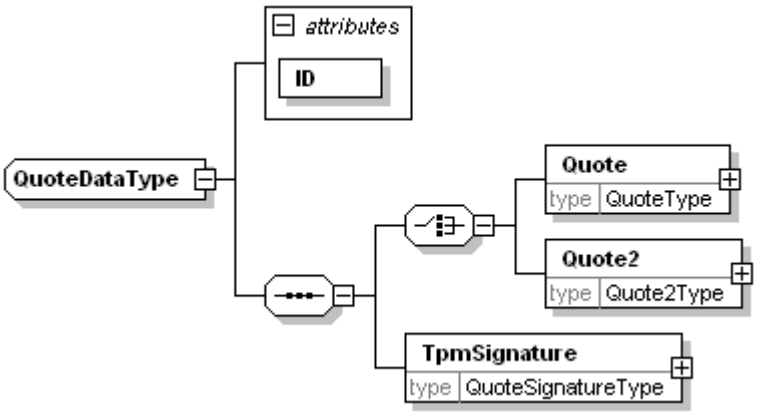
The QuoteDataType complex type 1.1b contains all of the data quote-related data in an integrity report. A 1.1b TPM only supports the Quote command, thus the Quote2 element may not be instantiated for 1.1b TPMs. A 1.2 TPM supports both the Quote and Quote2 commands, thus either of one the Quote or Quote2 elements may be instantiated. The Quote2 command is an optional command in the TPM 1.2 specification [2], thus it will be necessary to instantiate the Quote element for 1.2 TPMs that do not implement the Quote2 command. However, the Quote2 command is mandatory in the PC Client specifications.

Elements included in a QuoteDataType complex type are:

- Quote – Data returned from a call to the TPM Quote command including data necessary to compute and validate the quote signature, except for the signature itself.
- Quote2 - Data returned from a call to the TPM Quote2 command including data necessary to compute and validate the quote signature, except for the signature itself.
- TpmSignature – Contains the quote signature and all quote key information.

3.1.7.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **Quote** **Quote2** **TpmSignature**

used by element **ReportType/QuoteInfo**

attributes

Name	Type	Use	Default	Fixed
ID	xs:ID	required		

3.1.7.3 Attribute Detail

Attribute	Description
ID	Integrity Report document unique Record instance identifier. ID can be used in other parts of the document and by external systems to reference the quote instance in an integrity report.

3.1.7.4 XML

source

```
<xs:complexType name="QuoteDataType">
  <xs:sequence>
    <xs:choice>
      <xs:element name="Quote" type="QuoteType"/>
      <xs:element name="Quote2" type="Quote2Type"/>
    </xs:choice>
    <xs:element name="TpmSignature" type="QuoteSignatureType"/>
  </xs:sequence>
  <xs:attribute name="ID" type="xs:ID" use="required"/>
</xs:complexType>
```

3.1.8 complexType QuoteInfo2Type

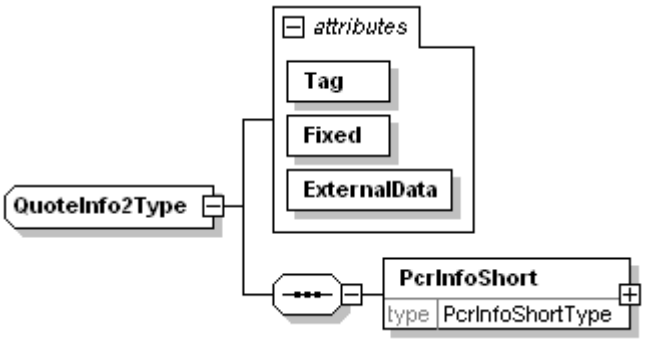
3.1.8.1 Description

The QuoteInfo2Type complex type is an XML representation of the 1.2 TPM's TPM_QUOTE_INFO2 structure. The Quote2 command returns PcrInfoShort, but does not return the attributes in QuoteInfo2Type. However, these attributes are used in the computation of the Quote2 signature, thus they are included so that a verifier can compute and validate the Quote2 signature.

QuoteInfo2Type includes the PcrInfoShort element. This element renders the TPM_PCR_INFO_SHORT structure returned by the Quote2 command.

3.1.8.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **PcrInfoShort**

used by element **Quote2Type/QuoteInfo2**

attributes

Name	Type	Use	Default	Fixed
Tag	xs:unsignedShort	required		
Fixed	xs:normalizedString	required		
ExternalData	xs:base64Binary	required		

3.1.8.3 Attribute Detail

Attribute	Description
Tag	From the TPM_QUOTE_INFO2 structure, the TPM specifications state this attribute is TPM_TAG_QUOTE_INFO2 which has a value of: 0x0036
Fixed	From the TPM_QUOTE_INFO2 structure, the TPM specifications state this attribute is the string “QUT2’
ExternalData	From the TPM_QUOTE_INFO2 structure, the TPM specifications state this attribute is 160 bits of externally supplied data – usually a freshness nonce

3.1.8.4 XML

source

```
<xs:complexType name="QuoteInfo2Type">
  <xs:sequence>
    <xs:element name="PcrInfoShort" type="PcrInfoShortType"/>
  </xs:sequence>
  <xs:attribute name="Tag" type="xs:unsignedShort" use="required"/>
  <xs:attribute name="Fixed" type="xs:normalizedString" use="required"/>
  <xs:attribute name="ExternalData" type="xs:base64Binary" use="required"/>
</xs:complexType>
```

3.1.9 complexType QuoteInfoType

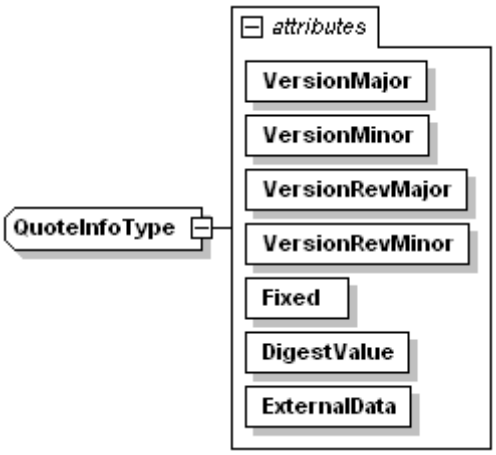
3.1.9.1 Description

The QuoteInfoType complex type is an XML representation of a 1.1b or 1.2 TPM’s TPM_QUOTE_INFO structure. The Quote command returns a TPM_PCR_COMPOSITE structure, but does not return the attributes in QuoteInfoType. However, these attributes are used in the computation of the Quote signature, thus they are included so that a verifier can compute and validate the Quote signature.

The first 4 attributes comprise the TPM’s TPM_STRUCT_VER structure and are 1.1.0.0. Refer to [2] for definition of TPM structures.

3.1.9.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

used by element **QuoteType/QuoteInfo**

attributes

Name	Type	Use	Default	Fixed
VersionMajor	xs:unsignedByte	required		
VersionMinor	xs:unsignedByte	required		
VersionRevMajor	xs:unsignedByte	required		
VersionRevMinor	xs:unsignedByte	required		
Fixed	xs:normalizedString	required		
DigestValue	**ds:DigestValueType**	required		
ExternalData	xs:base64Binary	required		

3.1.9.3 Attribute Detail

Attribute	Description
VersionMajor	From the TPM_QUOTE_INFO structure's TPM_STRUCT_VER, the TPM specifications state this attribute has a value of 0x01.
VersionMinor	From the TPM_QUOTE_INFO structure's TPM_STRUCT_VER, the TPM specifications state this attribute has a value of 0x01.
VersionRevMajor	From the TPM_QUOTE_INFO structure's TPM_STRUCT_VER, the TPM specifications state this attribute has a value of 0x00.
VersionRevMinor	From the TPM_QUOTE_INFO structure's TPM_STRUCT_VER, the TPM specifications state this attribute has a value of 0x00.
Fixed	From the TPM_QUOTE_INFO structure, the TPM specifications state this attribute is the string 'QUOT'.
DigestValue	From the TPM_QUOTE_INFO structure, the TPM specifications state this attribute is the result of the composite hash algorithm using the current value of the requested PCR indices.
ExternalData	From the TPM_QUOTE_INFO structure, the TPM specifications state this attribute is 160 bits of externally supplied data – usually a freshness nonce.

3.1.9.4 XML

source

```
<xs:complexType name="QuoteInfoType">
  <xs:attribute name="VersionMajor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="VersionMinor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="VersionRevMajor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="VersionRevMinor" type="xs:unsignedByte" use="required"/>
  <xs:attribute name="Fixed" type="xs:normalizedString" use="required"/>
  <xs:attribute name="DigestValue" type="ds:DigestValueType" use="required"/>
  <xs:attribute name="ExternalData" type="xs:base64Binary" use="required"/>
</xs:complexType>
```

3.1.10 complexType QuoteSignatureType

3.1.10.1 Description

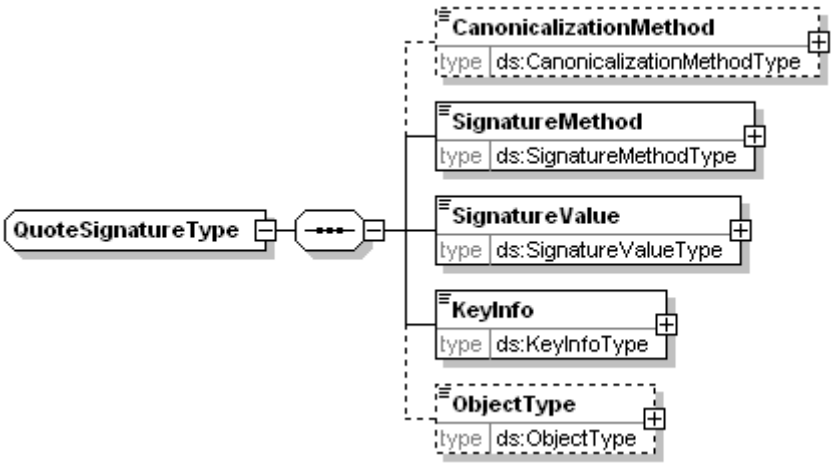
The QuoteSignatureType complex type contains the quote signature from either the TPM Quote or Quote2 command, information about the key used to quote PCRs, and any other data necessary to determine how to calculate the quote signature value.

Elements of QuoteSignatureType include:

- CanonicalizationMethod – This element defines the canonicalization algorithm used to create the signature. The method of calculating the TPM's quote signature is enforced in the TPM specification [4] and thus not germane to TPM 1.1b or 1.2 Quote structures and thus it is an optional element. However, it is included in order to leverage the XML signature structures and provide for future expansion in case future TPMs support a CanonicalizationMethod.
- SignatureMethod - Describes the signature algorithm used in the quote signature calculation.
- SignatureValue - Contains the TPM Quote or Quote2 signature. The Id attribute can be used to directly reference the signature value.
- Key Info - Describes the public key and its metadata used for the TPM Quote operation. For a 1.1b or 1.2 TPM, the following elements are germane: KeyName, KeyValue, and X509Data
- ObjectType – Optional element that describes any special encoding used in the signature process.

3.1.10.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **CanonicalizationMethod** **SignatureMethod** **SignatureValue** **KeyInfo** **ObjectType**

used by element **QuoteDataType/TpmSignature**

3.1.10.3 XML

source

```
<xs:complexType name="QuoteSignatureType">
  <xs:sequence>
    <xs:element name="CanonicalizationMethod" type="ds:CanonicalizationMethodType" minOccurs="0"/>
    <xs:element name="SignatureMethod" type="ds:SignatureMethodType"/>
    <xs:element name="SignatureValue" type="ds:SignatureValueType"/>
```

```
    <xs:element name="KeyInfo" type="ds:KeyInfoType"/>
    <xs:element name="ObjectType" type="ds:ObjectType" minOccurs="0"/>
   </xs:sequence>
  </xs:complexType>
```

3.1.11 complexType QuoteType

3.1.11.1 Description

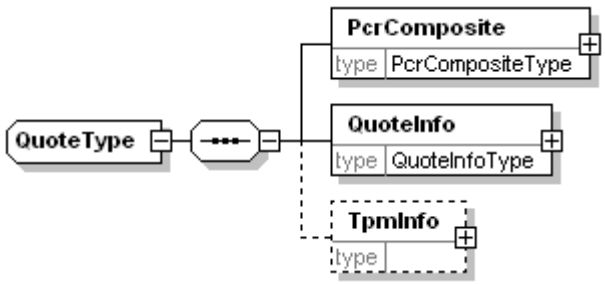
The QuoteType complex type is used to detail the data used by the TPM to calculate the Quote signature plus information describing the TPM. The Quote signature is included in the QuoteSignatureType complex type. The Quote command may be called on both a 1.1b TPM as well as on a 1.2 TPM. Elements of QuoteType complex type include:

- PcrComposite - This data is the only data output by the Quote command in addition to the signature itself. This data details which PCRs were quoted and their values.
- QuoteInfo – This data is not output from the TPM, but the structure is created in the TPM and used in the calculation of the Quote signature. It must be reconstructed in order to verify the Quote signature. It contains both the composite hash value and the externally supplied nonce.
- TpmInfo – TpmInfo is optional data describing the TPM used to create Quote data that may be useful in case there are any vendor-specific differences in rendering the Quote signature.

Refer to [2] for definition of TPM structures.

3.1.11.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **PcrComposite** **QuoteInfo** **TpmInfo**

used by element **QuoteDataType/Quote**

3.1.11.3 XML

source

```
<xs:complexType name="QuoteType">
 <xs:sequence>
  <xs:element name="PcrComposite" type="PcrCompositeType"/>
  <xs:element name="QuoteInfo" type="QuoteInfoType"/>
  <xs:element name="TpmInfo" minOccurs="0">
   <xs:complexType>
    <xs:choice>
     <xs:element name="CapVersionInfo" type="CapVersionInfoType"/>
     <xs:element name="TpmManufacturer" type="xs:base64Binary"/>
    </xs:choice>
   </xs:complexType>
  </xs:element>
 </xs:sequence>
</xs:complexType>
```

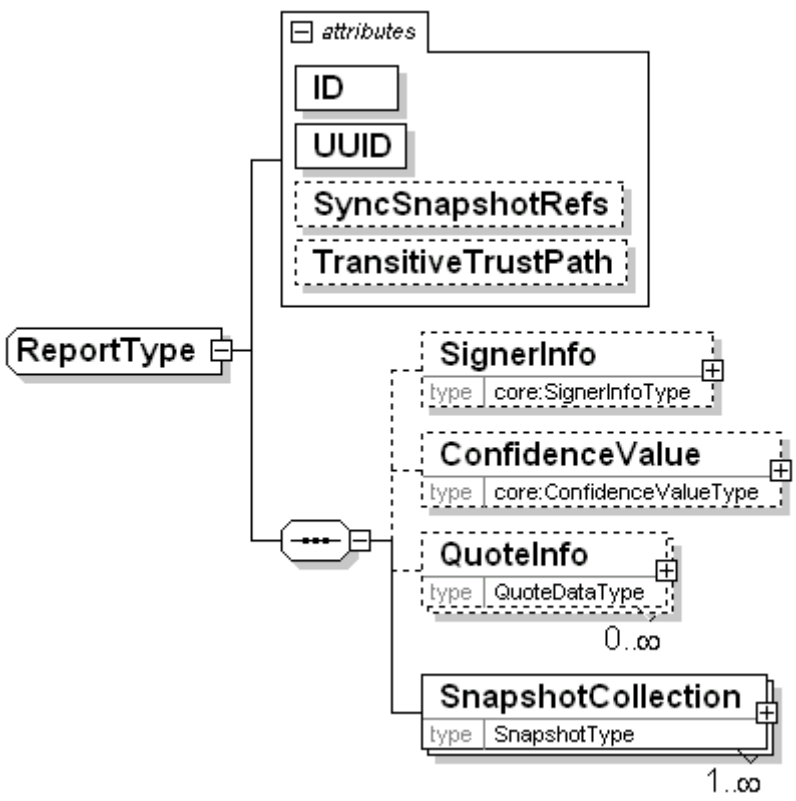
3.1.12 complexType ReportType

3.1.12.1 Description

The ReportType complex type defines an integrity report. The integrity report MUST contain one or more snapshots in the SnapshotCollection elements. Integrity reports should include either a TPM Quote or Quote2 attestation of PCRs or a Signature over the integrity report or both. If both are missing then a verifier will not be able to verify that the data included in the integrity report is authentic. Elements include:

- SignerInfo – The signature over the integrity report plus all information describing the key used to create the signature value. This element also optionally includes a confidence value and a time stamp designating when the integrity report was created and signed. Also included are Nonce and DateTime attributes. The Nonce is provided by the verifier as a means of ensuring the integrity report is fresh. The DateTime is when the integrity report was created (i.e. the data and time as obtained by the component constructing the integrity report).This element is defined by the core:SignerInfo complex type [1].
- ConfidenceValue – a numerical representation of trust to identify the level of confidence with which to trust the entire integrity report. This element is defined by the core:ConfidenceValue complex type [1].
- QuoteInfo – The TPM Quote or Quote2 signature, all data required by a verifier to calculate and verify the quote signature, and all the data describing the key used to create the quote signature.
- SnapshotCollection – The collection of all snapshots included in the integrity report. These elements are defined by the SnapshotType complex type.

3.1.12.2 Diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

children **SignerInfo ConfidenceValue QuoteInfo SnapshotCollection**

used by element **Report**

attributes

Name	Type	Use	Default	Fixed
ID	xs:ID	required		
UUID	xs:NMTOKEN	required		
SyncSnapshotRefs	xs:IDREFS	optional		
TransitiveTrustPath	xs:IDREFS	optional		

3.1.12.3 Attribute Detail

Attribute	Description
ID	Integrity Report document unique Record instance identifier. ID can by external systems to reference the integrity report.
UUID	Universally unique identifier for the report – allows external systems to reference this report
SyncSnapshotRefs	References to the Sync Snapshots
TransitiveTrustPath	References to the set of snapshots that comprise the transitive trust path

3.1.12.4 XML

source

```
<xs:complexType name="ReportType">
 <xs:sequence>
  <xs:element name="SignerInfo" type="core:SignerInfoType" minOccurs="0"/>
  <xs:element name="ConfidenceValue" type="core:ConfidenceValueType" minOccurs="0"/>
  <xs:element name="QuoteInfo" type="QuoteDataType" minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="SnapshotCollection" type="SnapshotType" maxOccurs="unbounded"/>
 </xs:sequence>
 <xs:attribute name="ID" type="xs:ID" use="required"/>
 <xs:attribute name="UUID" type="xs:NMTOKEN" use="required"/>
 <xs:attribute name="SyncSnapshotRefs" type="xs:IDREFS"/>
 <xs:attribute name="TransitiveTrustPath" type="xs:IDREFS"/>
</xs:complexType>
```

3.1.13 complexType SnapshotType

3.1.13.1 Description

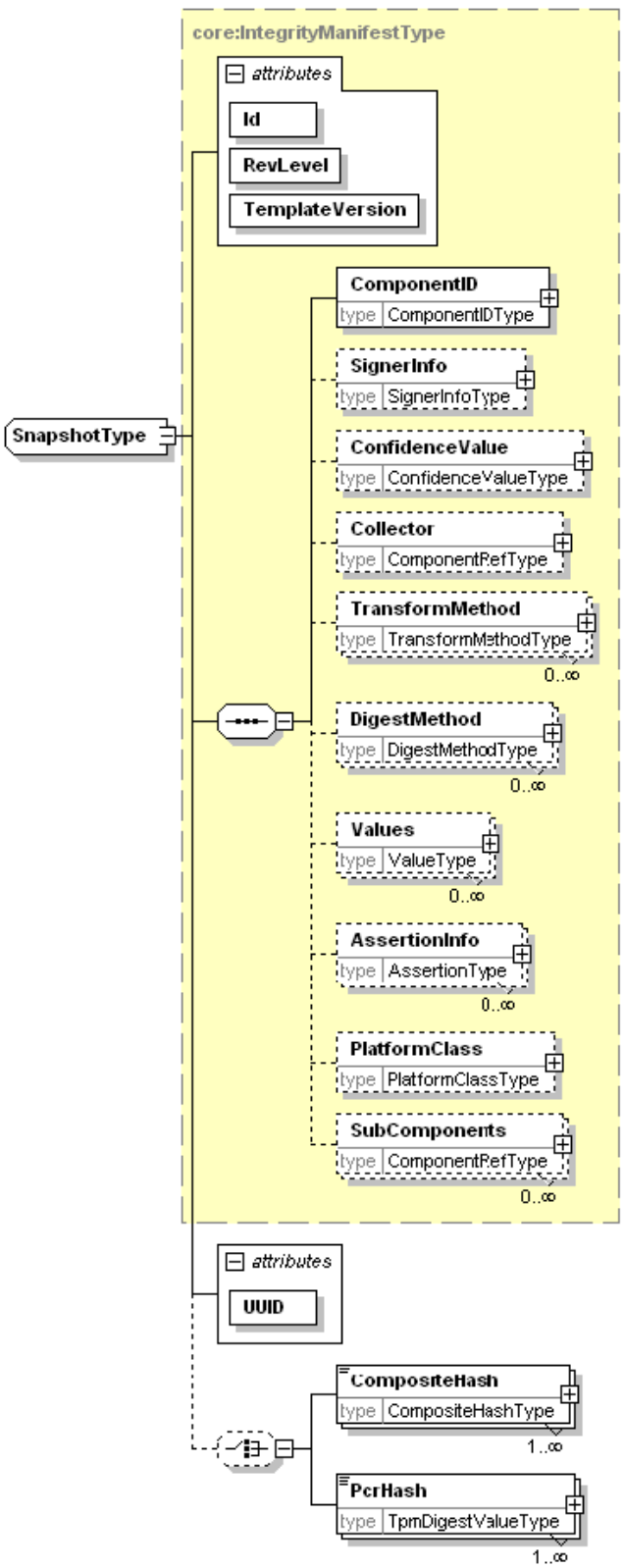
The SnapshotType complex type is used to describe integrity attributes of program code, discrete logic and collections of components. Any element that can be placed under change control is a candidate for being described using the SnapshotType complex type. SnapshotType complex type inherits its structure from Core:IntegrityManifestType complex type [1] and adds a UUID attribute and choice of CompositeHash or PcrHash digest structures.

Elements of SnapshotType include:

- ComponentID – is a unique complex identifier linking the component to a change management process. For a sync snapshot (a snapshot whereby the PcrHash value is a PCR value - see [8]), the ComponentID SHOULD be the Vendor GUID of the component that constructed the snapshot (i.e. PTS). Version 2.0 of this specification adds the additional required attributes for ComponentVendorID and FunctionalComponentID. ComponentVendorID is a 24-bit SMI value for the vendor. FunctionalComponentID is the 64-bit Integer ID associated with the functional component itself.
- SignerInfo – is a signature over the Snapshot. It includes information about the entity that produced the signature. A single signature may be applied.
- ConfidenceValue – a numerical representation of trust to identify the level of confidence with which to trust the integrity values (Values) and assertions (AssertionInfo) in the snapshot.

- Collector – is a reference to the utility (component) used to construct the snapshot. A snapshot for the Collector may be separately obtained to find information relating to the environment that produced *this* snapshot. A single collector may be referenced.
- TransformMethod – contains algorithm identifiers for transforms that may have been applied prior to applying a digest method. Multiple transformation methods may be defined.
- DigestMethod – contains algorithm identifiers for hash algorithms that are used to compute message digests. Multiple digest methods may be defined.
- Values – contains integrity measurements (message digests) that pertain to *this* component. It is reasonable (even desirable) that schemas capturing domain specific structure should incorporate a composite hash structure that is incorporated into the Snapshot CompositeHash or PcrHash. Multiple instances of Values elements may be supplied. If TransformMethod and DigestMethod are not populated, then Values MUST include these structures. ValuesType as defined in the core integrity schema [1] is intended to be extended with one or more schemas such as the Simple Object Schema [9].
- AssertionInfo – contains domain specific description of attributes affecting quality, assurance or reliability assessments, but where it isn't possible for measurement engines to collect *actual* values. Multiple instances of AssertionInfo elements may be supplied. AssertionInfo as defined in the core integrity schema [1] is to be extended with one or more schemas such as the Quality Qualities Schema [10].
- PlatformClass – identifies the type of platform that integrity values pertain to. In particular, the methodology for PCR allocation is specified by platform specific specifications.
- SubComponents – are references to finer grain components that make up *this* component.
- CompositeHash – contains a composite hash calculation of elements in a Snapshot. This element MUST be populated if the snapshot does not detail a PCR (i.e. not a sync snapshot). It SHOULD be included in the hash calculation for the snapshot signature. The schema allows for multiple CompositeHash elements; however more than one CompositeHash elements SHOULD only be included if more than one digest method is used within the snapshot. If a composite hash is not included and a signature is included, the integrity value for the snapshot is taken to be the signature hash. CompositeHash and PcrHash are mutually exclusive, but a snapshot may not have either one.
- PcrHash – contains a composite hash calculation of elements in a Snapshot. This element MUST be populated if the snapshot details a PCR (i.e. it is a sync snapshot). It SHOULD be included in the hash calculation for the snapshot signature. It is used to correlate a composite hash to a TPM PCR value. The schema allows for multiple PcrHash elements; this feature is included for future expansion as the current PTS specification only uses a single TPM PCR and thus only a single PcrHash element SHOULD be included in a snapshot. If a PcrHash is not included, the integrity value for the snapshot is taken to be the signature hash. CompositeHash and PcrHash are mutually exclusive, but a snapshot may not have either one.

3.1.13.2 Diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type extension of **core:IntegrityManifestType**

properties base core:IntegrityManifestType

children **ComponentID** **SignerInfo** **Collector** **TransformMethod** **DigestMethod** **Values** **AssertionInfo** **PlatformClass** **SubComponents** **CompositeHash** **PcrHash**

Used by elements **Snapshot** **ReportType/SnapshotCollection**

attributes

Name	Type	Use	Default	Fixed
ID	xs:ID	required		
RevLevel	xs:integer	required		
UUID	xs:NMTOKEN	required		
TemplateVersion	xs:integer	required		

3.1.13.3 Attribute Detail

Attribute	Description
ID	Snapshot unique record instance identifier. ID can be used in other parts of the document and by external systems to reference the snapshot instance in an integrity report.
RevLevel	RevLevel is a revision number (increment for more recent revision) to distinguish revisions of an integrity manifest structure. RevLevel applies to instances of snapshot structures having the same ID value. This is how a verifier can determine if a snapshot has the full desired structure for its verification process.
UUID	Globally unique identifier to allow XML documents, external systems and this XML document to refer to a snapshot instance
TemplateVersion	TemplateVersion indicates the revision of the structure of this Integrity Manifest. All new Integrity Manifests should use a 1 in this field and each time the structure of the Integrity Manifest changes, this field should be incremented. The structure indicates the organization of component/sub-component hierarchy described by the document. If a new component is added or the sub-component set changes this reflects a different organization of the document. This field is used during attestation to detect when the two parties have the same Integrity Manifest so it can be used as the basis for organizing the resulting Integrity Report.

3.1.13.4 XML

source

```
<xs:complexType name="SnapshotType">
  <xs:complexContent>
    <xs:extension base="core:IntegrityManifestType">
      <xs:sequence minOccurs="0">
        <xs:choice>
          <xs:element name="PcrHash" type="TpmDigestValueType" maxOccurs="unbounded"/>
          <xs:element name="CompositeHash" type="CompositeHashType" maxOccurs="unbounded"/>
        </xs:choice>
      </xs:sequence>
      <xs:attribute name="UUID" type="xs:NMTOKEN" use="required"/>
      <xs:attribute name="TemplateVersion" type="xs:integer" use="required"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

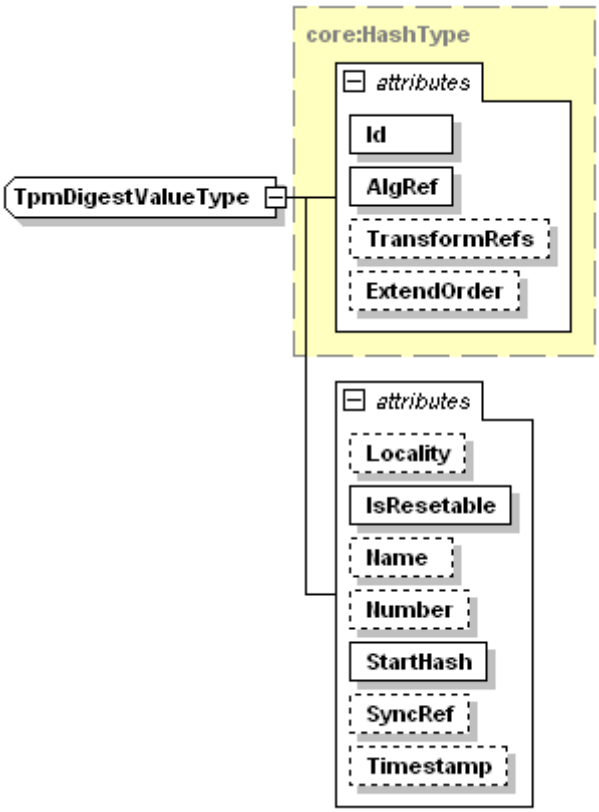
3.1.14 complexType TpmDigestValueType

3.1.14.1 Description

The TpmDigestValueType complex type is an extension of the core:HashType complex type defined in [1]. This is the end digest value in a snapshot of the values referenced by the ExtendOrder attribute. TpmDigestValueType extends core:Hash type by adding the following optional attributes: Locality IsResetable, Name, Number, StartHash, SyncRef, and TimeStamp. TpmDigestValueType complex type MUST be used for PCR digests (instead of CompositeHashType complex type).

3.1.14.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type extension of **core:HashType**

properties base core:HashType

used by element **SnapshotType/PcrHash**

attributes

Name	Type	Use	Default	Fixed
Id	xs:ID	required		
AlgRef	xs:IDREF	required		
TransformRefs	xs:IDREFS	optional		
ExtendOrder	xs:IDREFS	optional		
Locality	xs:integer	optional		
IsResetable	xs:boolean	required		
Name	xs:normalizedString	optional		
Number	xs:integer	optional		
StartHash	ds:DigestValueType	required		
SyncRef	xs:IDREF	optional		
Timestamp	xs:dateTime	optional		

3.1.14.3 Attribute Detail

Attribute	Description
Id	TPM PCR Digest unique record instance identifier. ID can be used in other parts of the document and by external systems to reference the snapshot instance in an integrity report.
AlgRef	AlgRef refer to a hash algorithm as defined by DigestMethodType
TransformRefs	TransformRefs Refers to transformation functions defined by TransformMethod elements of type TransformMethodType.

ExtendOrder	ExtendOrder contains an ordered list of xs:IDREF values. Values at the beginning of the list occur before values at the end. Therefore, the first entry in the list would be the first value extended, the last entry would be the last value extended.
Locality	The locality indicator for the TPM PCR.
IsResetable	IsResetable indicates whether it is possible to reset the TPM PCR without rebooting the platform.
Name	Friendly name assigned to the TPM PCR – this reference provides a reference to the TPM PCR that is meaningful to a human.
Number	Number is the PCR number that is recognized by the TPM
StartHash	The initial digest value of the TPM PCR prior to extending values.
SyncRef	Reference (xs:IDREF) to the Id of the sync snapshot.
Timestamp	Time stamp when the snapshot was completed.

3.1.14.4 XML

source

```
<xs:complexType name="TpmDigestValueType">
  <xs:simpleContent>
    <xs:extension base="core:HashType">
      <xs:attribute name="Locality" type="xs:integer"/>
      <xs:attribute name="IsResetable" type="xs:boolean" use="required"/>
      <xs:attribute name="Name" type="xs:normalizedString"/>
      <xs:attribute name="Number" type="xs:integer"/>
      <xs:attribute name="StartHash" type="ds:DigestValueType" use="required"/>
      <xs:attribute name="SyncRef" type="xs:IDREF"/>
      <xs:attribute name="Timestamp" type="xs:dateTime"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

3.2 ELEMENTS

3.2.1 element PcrCompositeType/PcrSelection

3.2.1.1 Description

PcrSelection element is a single instance of PcrSelectionType - see section 3.1.5. The contents specify which PCRs are Quoted in an Integrity Report.

3.2.1.2 XML

source

```
<xs:element name="PcrSelection" type="PcrSelectionType"/>
```

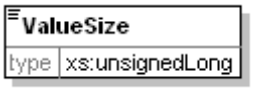
3.2.2 element PcrCompositeType/ValueSize

3.2.2.1 Description

ValueSize is the total size in bytes of the array of PcrValue structures in PcrCompositeType (see 3.1.3).

3.2.2.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type xs:unsignedLong

properties isRef 0
content simple

3.2.2.3 XML

source

```
<xs:element name="ValueSize" type="xs:unsignedLong"/>
```

3.2.3 element PcrCompositeType/PcrValue

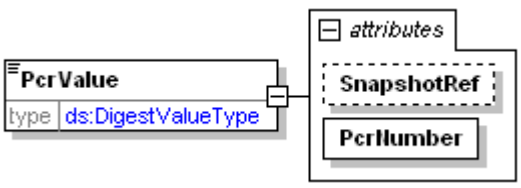
3.2.3.1 Description

The Pcrvalue element extends the XML W3C DigestValueType [3] simple type by adding the SnapshotRef and PcrNumber attributes. The PcrValue element is a single PCR digest value in a Quote. The Array of PcrValue structures (see PcrCompositeType 3.1.3) details the combination of PCR digest values for all PCRs chosen for the Quote.

The mandatory PcrNumber attribute allows the recipient of an array of PcrValue structures to map this digest value with the corresponding PCR from the PcrSelection structure (see 3.2.1) in PcrCompositeType. The optional SnapshotRef is a reference to the corresponding snapshot that has the same end hash value.

3.2.3.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type extension of **ds:DigestValueType**

properties
isRef 0
content complex

attributes

Name	Type	Use	Default	Fixed
SnapshotRef	xs:IDREF	optional		
PcrNumber	xs:unsignedLong	required		

3.2.3.3 Attribute Detail

Attribute	Description
SnapshotRef	SnapshotRef is an IDREF reference to the snapshot that has this PCR value as it's end digest value.
PcrNumber	PcrNumber is the TPM's identifier for the PCR.

3.2.3.4 XML

source

```
<xs:element name="PcrValue" maxOccurs="unbounded">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="ds:DigestValueType">
        <xs:attribute name="SnapshotRef" type="xs:IDREF" use="optional"/>
        <xs:attribute name="PcrNumber" type="xs:unsignedLong" use="required"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
```

3.2.4 element PcrInfoShortType/PcrSelection

3.2.4.1 Description

PcrSelection element is a single instance of PcrSelectionType (see section 3.1.5). The contents specify which PCRs are Quoted in an Integrity Report.

3.2.4.2 XML

source

```
<xs:element name="PcrSelection" type="PcrSelectionType"/>
```

3.2.5 element PcrInfoShortType/LocalityAtRelease

3.2.5.1 Description

The LocalityAtRelease element is a single unsigned byte that specifies the locality modifier to provide the requestor a more complete view of the current (while Quoting) platform configuration. This is a mandatory element of complex type PcrInfoShortType (see 3.1.4) and the data is required to validate the Quoted digest value.

3.2.5.2 Diagram

diagram

namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type xs:unsignedByte

properties
isRef 0
content simple

3.2.5.3 XML

source

```
<xs:element name="LocalityAtRelease" type="xs:unsignedByte"/>
```

3.2.6 element PcrInfoShortType/CompositeHash

3.2.6.1 Description

The CompositeHash element is defined by the XML W3C DigestValueType simple type [3] and is a digest of the PcrInfoShortType/PcrComposite structure.

3.2.6.2 Diagram

diagram

namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type **ds:DigestValueType**

properties
isRef 0
content simple

3.2.6.3 XML

source

```
<xs:element name="CompositeHash" type="ds:DigestValueType"/>
```

3.2.7 element PcrInfoShortType/PcrComposite

3.2.7.1 Description

The PcrComposite element is defined by the PcrCompositeType complex type (see 3.1.3). It is not part of a TPM PCR_INFO_SHORT structure; however CompositeHash is a hash of PcrComposite, thus PcrComposite is included in PcrInfoShortType to provide the necessary detail used to compute CompositeHash.

3.2.7.2 XML

source

```
<xs:element name="PcrComposite" type="PcrCompositeType"/>
```

3.2.8 element Quote2Type/CapVersionInfo

3.2.8.1 Description

The CapVersionInfo element is defined by the CapVersionInfoType complex type (see 3.1.1). The 1.2 TPM Quote2 command supports an optional request to return CapVersionInfo and include it in the quoted digest calculation. It is optional in Quote2Type complex type (see 3.1.6) since it is optional in the TPM Quote2 command.

3.2.8.2 XML

source

```
<xs:element name="CapVersionInfo" type="CapVersionInfoType" minOccurs="0"/>
```

3.2.9 element Quote2Type/QuoteInfo2

3.2.9.1 Description

The QuoteInfo2 element is defined by the QuoteInfo2Type complex type (see 3.1.8). This is the non-optional output from a TPM Quote command.

3.2.9.2 XML

Source

```
<xs:element name="QuoteInfo2" type="QuoteInfo2Type"/>
```

3.2.10 element QuoteDataType/Quote

3.2.10.1 Description

The Quote element is defined by the QuoteType complex type (see 3.1.11).

3.2.10.2 XML

source
```
<xs:element name="Quote" type="QuoteType"/>
```

3.2.11 element QuoteDataType/Quote2

3.2.11.1 Description

The Quote2 element is defined by the Quote2Type complex type (see 3.1.6).

3.2.11.2 XML

source
```
<xs:element name="Quote2" type="Quote2Type"/>
```

3.2.12 element QuoteDataType/TpmSignature

3.2.12.1 Description

The TpmSignature element is defined by the QuoteSignatureType complex type (see 3.1.10). This structure contains the Quote signature value and information describing the key used and method of signature computation.

3.2.12.2 XML

source
```
<xs:element name="TpmSignature" type="QuoteSignatureType"/>
```

3.2.13 element QuoteInfo2Type/PcrInfoShort

3.2.13.1 Description

The PcrInfoShort element is defined by the PcrInfoShortType complex type (see 3.1.4).

3.2.13.2 XML

source
```
<xs:element name="PcrInfoShort" type="PcrInfoShortType"/>
```

3.2.14 element QuoteSignatureType/CanonicalizationMethod

3.2.14.1 Description

The CanonicalizationMethod element is defined by the XML W3C CononiicalizationMethodType complex type [3] and specifies the canonicalization algorithm used to create a signature. The method of calculating the TPM's quote signature is enforced in the TPM specification [4] and thus not germane to TPM 1.1b or 1.2 Quote structures, thus it is an optional element. However, it is included in order to leverage the XML signature structures and provide for future expansion in case TPMs support CanonicalizationMethod.

3.2.14.2 XML

source
```
<xs:element name="CanonicalizationMethod" type="ds:CanonicalizationMethodType"/>
```

3.2.15 element QuoteSignatureType/KeyInfo

3.2.15.1 Description

The KeyInfo element is defined by the XML W3C KeyInfoType complex type [3] and describes the keys used for the TPM Quote operation. For a 1.1b or 1.2 TPM, the following elements are germane:

- KeyName – String name for the Quote key
- KeyValue – The RSA Quote key modulus and exponent (the public key)
- X509Data – Certificate data for the Quote key

3.2.15.2 XML

source

```
<xs:element name="KeyInfo" type="ds:KeyInfoType"/>
```

3.2.16 element QuoteSignatureType/ObjectType

3.2.16.1 Description

The ObjectType element is defined by the XML W3C ObjectType complex type [3]. Use of this element is optional and describes any special encoding used in the signature process.

3.2.16.2 XML

source

```
<xs:element name="ObjectType" type="ds:ObjectType" minOccurs="0"/>
```

3.2.17 element QuoteSignatureType/SignatureMethod

3.2.17.1 Description

The SignatureMethod element is defined by the XML W3C SignatureMethodType complex type [3] and describes signature algorithm used in the quote signature calculation.

3.2.17.2 XML

source

```
<xs:element name="SignatureMethod" type="ds:SignatureMethodType"/>
```

3.2.18 element QuoteSignatureType/SignatureValue

3.2.18.1 Description

The SignatureValue element is defined by the XML W3C SignatureValueType complex type [3] and contains the TPM Quote or Quote2 signature. The Id attribute can be used to directly reference the signature value.

3.2.18.2 XML

source

```
<xs:element name="SignatureValue" type="ds:SignatureValueType"/>
```

3.2.19 element QuoteType/PcrComposite

3.2.19.1 Description

The PcrComposite element is defined by the PcrCompositeType complex type (see 3.1.3)

3.2.19.2 XML

source
```
<xs:element name="PcrComposite" type="PcrCompositeType"/>
```

3.2.20 element QuoteType/QuoteInfo

3.2.20.1 Description

The QuoteInfo element is defined by the QuoteInfoType complex type (see 3.1.9).

3.2.20.2 XML

source
```
<xs:element name="QuoteInfo" type="QuoteInfoType"/>
```

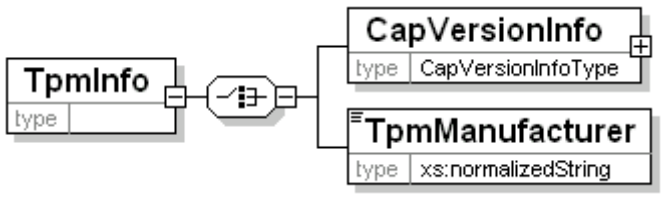
3.2.21 element QuoteType/TpmInfo

3.2.21.1 Description

The TpmInfo element – TpmInfo is optional data identifying the TPM used to create Quote data in the QuoteType complex type (see 3.1.11). This information may be useful in case there are any vendor-specific differences in rendering the Quote signature. If the TPM is a 1.1b TPM, then TpmManufacturer should be instantiated from a call to the TPM GetCapability command. If the TPM is a 1.2 TPM, then CapVersionInfo should be instantiated from a call to the TPM GetCapability command.

3.2.21.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

properties
isRef 0
content complex

children **CapVersionInfo** **TpmManufacturer**

3.2.21.3 XML

source
```
<xs:element name="TpmInfo" minOccurs="0">
  <xs:complexType>
    <xs:choice>
      <xs:element name="CapVersionInfo" type="CapVersionInfoType"/>
      <xs:element name="TpmManufacturer" type="xs:normalizedString"/>
    </xs:choice>
  </xs:complexType>
</xs:element>
```

3.2.22 element QuoteType/TpmInfo/CapVersionInfo

3.2.22.1 Description

The CapVersionInfo element is defined by the CapVersionInfoType complex type (see 3.1.1). There are no additional context dependent semantics.

3.2.22.2 XML

source <xs:element name="CapVersionInfo" type="CapVersionInfoType"/>

3.2.23 element QuoteType/TpmInfo/TpmManufacturer

3.2.23.1 Description

The TpmManufacturer element is defined by the XML W3C normalizedString simple type [3]. The TpmManufacturer element should be instantiated in a TpmInfo element (see 3.2.21) if the TPM is a 1.1b TPM. The content is the result of calling the TPM GetCapability command and requesting the CAP_PROP_MANUFACTURER for a 1.1b or 1.2 TPM. The value returned is a UInt32 and must be converted into a string of 4 bytes with any following NULL bytes removed. Alternatively this data may be retrieved by calling the TPM GetCapability command and requesting CAP_VERSION_INFO for a 1.2 TPM and using the tpmVendorID field. The TPM returns the same string for both calls. This is a 4-byte value that is usually the vendor's stock ticker value in capitalized characters. If the string is less than 4 bytes long, it must be padded with trailing NULLs prior to use.

3.2.23.2 Diagram

diagram

namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#

type **xs:normalizedString**

properties
isRef 0
content simple

3.2.23.3 XML

source <xs:element name="TpmManufacturer" type="xs:normalizedString"/>

3.2.24 element Report

3.2.24.1 Description

The Report element is defined by the ReportType complex type (see 3.1.12). This is an integrity report. There are no additional context dependent semantics.

3.2.24.2 XML

source <xs:element name="Report" type="ReportType"/>

3.2.25 element ReportType/QuoteInfo

3.2.25.1 Description

The QuoteInfo element is defined by the QuoteDataType complex type (see 3.1.7). This structure contains all of the quote-related data for the integrity report. There are no additional context dependent semantics.

3.2.25.2 XML

source <xs:element name="QuoteInfo" type="QuoteDataType" minOccurs="0" maxOccurs="unbounded"/>

3.2.26 element ReportType/SnapshotCollection

3.2.26.1 Description

The SnapshotCollection element is defined by the SnapshotType complex type (see 3.1.13). SnapshotCollection is an unbounded element containing all of the snapshots included in the integrity report.

3.2.26.2 XML

source
```
<xs:element name="SnapshotCollection" type="SnapshotType" maxOccurs="unbounded"/>
```

3.2.27 element SnapshotType/CompositeHash

3.2.27.1 Description

The CompositeHash element is defined by the CompositeHashType complex type (see 3.1.2). This is the final hash value of the snapshot after including all values and assertions. There should only be one CompositeHash element unless the snapshot utilizes more than one digest method.

3.2.27.2 XML

source
```
<xs:element name="CompositeHash" type="CompositeHashType" maxOccurs="unbounded"/>
```

3.2.28 element SnapshotType/PcrHash

3.2.28.1 Description

The PcrHash element is defined by the TpmDigestValueType complex type (see 3.1.14). This is the final hash value of the snapshot after including all values and assertions. There may only be a single PcrHash element for a 1.1b or 1.2 TPM for a PTS that may only utilize a single PCR (as the initial IF-PTS specification requires).

3.2.28.2 XML

source
```
<xs:element name="PcrHash" type="TpmDigestValueType" maxOccurs="unbounded"/>
```

3.2.29 element Snapshot

3.2.29.1 Description

The Snapshot element is defined by the SnapshotType complex type (see 3.1.13). There may be an unlimited number of Snapshot elements in an integrity report.

3.2.29.2 XML

source
```
<xs:element name="Snapshot" type="SnapshotType"/>
```

4 Appendix A – Example Integrity Report

The following XML is provided as an example integrity report. The integrity report document contains 2 snapshots and a Quote from a TPM using PCR #13. The data contained within the XML is provided for example purposes only and should not be interpreted as real data.

```
<?xml version="1.0" encoding="UTF-8"?>
<Report xmlns="http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/integrity_report#
Integrity_Report_Manifest_v17.xsd
http://www.trustedcomputinggroup.org/XML/SCHEMA/1_0/simple_object# SimpleObject_v4.xsd
http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/core_integrity# Core_Integrity_Manifest_v14.xsd"
xmlns:core="http://www.trustedcomputinggroup.org/XML/SCHEMA/2_0/core_integrity#"
xmlns:stuff="http://www.trustedcomputinggroup.org/XML/SCHEMA/1_0/simple_object#" ID="_C0136C73-93A9-4e4a-A056-
70BDFE4A4A46" SyncSnapshotRefs="_1901366E-1409-4eeb-99E1-1F4880034EEB" UUID="C0136C73-93A9-4e4a-A056-
70BDFE4A4A46">
        <QuoteInfo ID="_82897509-2D8A-4061-A2D9-DA2975998C70">
                <Quote>
                        <PcrComposite>
                                <PcrSelection SizeOfSelect="2" PcrSelect="AAQ="/>
                                <ValueSize>15</ValueSize>
                                <PcrValue PcrNumber="13">AqW6avizcmWIL0mTpWncin/NrPE=</PcrValue>
                        </PcrComposite>
                        <QuoteInfo VersionMinor="2" Fixed="QUOT"
                        ExternalData="BqW335izcmWIL0m09Wncin/NrPE="
                        DigestValue="AqW6avizcmWIL0mTpWncin/NrPE=" VersionMajor="1"
                        VersionRevMajor="1" VersionRevMinor="2"/>
                </Quote>
                <TpmSignature>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

        <SignatureValue>4Rxc/Nh/i6zYEumYbqhh8h+qTbGWowCKbEJgEH3rraxM1WMPYi3YdKR/D+2TNhBdPg3U7ydy6WwJ/
c6uULq7ywUREG0zjxY4Vxe4wxv269VXtXQNXwzPCwfVEVhbc+wJw6HE4fhX6y4FCx2D6
djD9r2geIBRil0IfrU=</SignatureValue>
                        <KeyInfo>
                                <KeyValue>
                                        <RSAKeyValue>

        <Modulus>6h6uowDi1q5LAEyD3ghOdZcS9+VlwFeFwu+C9z4MRyunpeFKl0nZ2qtE97LoxHfKBxa+LJsRGbLOeGxZc9w3
me0VZzQJ8LsrIrbG+Mvtk4eZkEQrF02tpC/zIMe30T4B0kpYkI91elpeMp/n1RWzUH8+a/5cWVUnHT80=</Modulus>
                                                <Exponent>AQAB</Exponent>
                                        </RSAKeyValue>
                                </KeyValue>
                        </KeyInfo>
                </TpmSignature>
        </QuoteInfo>
        <SnapshotCollection Id="_979ADB1F-E75B-4b94-9EFE-0FAD9C125549" RevLevel="0" UUID="979ADB1F-E75B-4b94-
9EFE-0FAD9C125549" TemplateVersion=”1”>
                <core:ComponentID Id="_4CD06805-5364-4d01-9722-BD3F2CA56788" SimpleName="Test Application">
                        <core:VendorID Name="Wave Systems Corp.">
                                <core:SmiVendorId>15997</core:SmiVendorId>
                        </core:VendorID>
                </core:ComponentID>
                <core:DigestMethod Id="sha1" Algorithm=""/>
                <core:Values>
                        <stuff:SimpleSnapshotObject>
                                <stuff:Objects Name="c:\program files\test.h">
                                        <stuff:Hash Id="_1092DFDD-2DDD-4cb1-A4A7-1A0C141E56FB"
AlgRef="sha1">7EbfD2FLhcDFxGdQE9/ZjskOGcw=</stuff:Hash>
                                </stuff:Objects>
                        </stuff:SimpleSnapshotObject>
                </core:Values>
```

```
                    <CompositeHash Id="_779ADB1F-E75B-4b94-9EFE-0FAD9C125549"
AlgRef="sha1">7EbfD2FLhcDFxGdQE9/ZjskOGcw=</CompositeHash>
            </SnapshotCollection>
            <SnapshotCollection Id="_1901366E-1409-4eeb-99E1-1F4880034EEB" RevLevel="0" UUID="1901366E-1409-4eeb-99E1-
1F4880034EEB" TemplateVersion=”1”>
                    <core:ComponentID Id="_234234" VersionBuild="4" VersionMajor="1" VersionMinor="2" SimpleName="PTS
Service" ModelSystemClass="NTRU">
                            <core:VendorID Name="Wave Systems">
                                    <core:SmiVendorId>15997</core:SmiVendorId>
                            </core:VendorID>
                    </core:ComponentID>
                    <core:Collector>
                            <core:ComponentID Id="a12345" VersionBuild="4" VersionMajor="1" VersionMinor="2"
SimpleName="PTS Service" ModelSystemClass="NTRU">
                                    <core:VendorID Name="Wave Systems">
                                            <core:SmiVendorId>15997</core:SmiVendorId>
                                    </core:VendorID>
                            </core:ComponentID>
                    </core:Collector>
                    <core:Values>
                            <stuff:SimpleSnapshotObject>
                                    <stuff:Objects Name="C:\Program Files\Wave Systems Corp\PTS\ptsserver.exe">
                                            <stuff:Hash Id="_D4D8A65C-EE5F-4693-BE21-56DE1BFC72DD"
AlgRef="sha1">7EbfD2FLhcDFxGdQE9/ZjskOGcw=</stuff:Hash>
                                    </stuff:Objects>
                                    <stuff:Objects Name="C:\Program Files\Wave Systems Corp\PTS\ptssdk.dll">
                                            <stuff:Hash Id="_32D24FF8-8D52-49cb-9C21-430233E81576"
AlgRef="sha1">7EbfD2FLhcDFxGdQE9/ZjskOGcw=</stuff:Hash>
                                    </stuff:Objects>
                            </stuff:SimpleSnapshotObject>
                    </core:Values>
                    <PcrHash IsResetable="false" Id="S29934" AlgRef="sha1" ExtendOrder="_1901366E-1409-4eeb-99E1-
1F4880034EEB" StartHash="7EbfD2FLhcDFxGdQE9/ZjskOGcw= ">
                            SinjXkRRXpIMteFROEGRtUxwa8=

                    </PcrHash>
            </SnapshotCollection>
</Report>
```

5 References

[1] Trusted Computing Group, TCG IWG Core Integrity Schema, Specification Version 2.0, September 2011

[2] Trusted Computing Group, TCG TPM Specification, TPM Main Part 2 TPM Structures, Specification version 1.2, Level 2, Revision 116, 3 June 2010.

[3] W3C, XML Schema, W3C Consortium, October 2004.

[4] Trusted Computing Group, TCG TPM Specification, TPM Main Part 3 Commands, Specification version 1.2, Level 2, Revision 116, 19 March 2010.

[5] Trusted Computing Group, TCG IWG Reference Manifest Schema, Specification Version 2.0, Revision 0.3, 15 September 2011.

[6] Trusted Computing Group, TCG IWG Architecture Part II, Specification Version 1.0, Revision 1.0, November 2006.

[7] Trusted Computing Group, *TNC Architecture for Interoperability*, Specification Version 1.1, May 1 2006.

[8] IF-PTS Specification.

[9] Trusted Computing Group, TCG IWG Simple Object Schema, Specification Version 1.0, Revision 1.0, September 2006.

[10] Trusted Computing Group, TCG IWG Security Qualities Schema, Specification Version 1.0, Revision 1.0, September 2006.

[11] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, Internet Engineering Task Force RFC 2119, March 1997.