SNMP MIB for TPM-Based Attestation

Specification Version 0.8
Revision 0.02
May 22, 2018
DRAFT

Contact: admin@trustedcomputinggroup.org

Work in Progress

This document is an intermediate draft for comment only and is subject to change without notice. Readers should not design products based on this document.

TCG Public Review

TCG

Disclaimers, Notices, and License Terms

1.1.1.1.1.1.1.1 Table of Contents

1.1.1.1.1.1.1.1 Table of Contents iii

Scope 1

1.2 Key words 1

1.3 Informative vs Normative Text 1

2. References 2

2.1 Normative references 2

3. Acronyms 3

4. Conformance 4

4.1 Introduction 4

4.2 SNMP Management - Normative 4

4.3 Security Considerations 4

4.3.1 Reconnaissance 4

4.3.2 SNMP 4

4.3.3 Key Properties 5

4.3.4 Legacy Compatibility 5

5. SNMP MIB Operation 6

5.1 MIB structure 6

5.2 Example of Attestation with SNMP 7

6. SNMP MIB – Normative 10

Scope

1.2 Key words

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document normative statements are to be interpreted as described in RFC-2119, *Key words for use in RFCs to Indicate Requirement Levels.*

1.3 Informative vs Normative Text

Normative text is specifically identified in this specification. A section marked as Normative is entirely Normative. If not marked Normative, the section is Informative.

2. References

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

1. Trusted Computing Group (TCG), "TPM Keys for Platform Identity for TPM 1.2", Version 1.0r3, May 2015
2. IETF Standard 58 (STD58):
    a. RFC-2578, Structure of Management Information, v2 (SMIv2)
    b. RFC-2579, Textual Conventions for SMIv2
    c. RFC-2580, Conformance Statements for SMIv2
3. IETF RFC-6933, Entity MIB, Version 4
4. IEEE Standard for Local and metropolitan area networks, 802.1AR: *Secure Device Identity*.
5. TPM Main Specification Revision 1.2, Part 1: Design Principles
6. TPM Main Specification Revision 1.2, Part 2: TPM Structures
7. TPM Main Specification Revision 1.2, Part 3: Commands
8. TCG Trusted Platform Module Library, Family 2.0, Part 1: Architecture.
9. TCG Trusted Platform Module Library, Family 2.0, Part 2: Structures.
10. TCG Trusted Platform Module Library, Family 2.0, Part 3: Commands.

3. Acronyms

The table below describes the acronyms used in this specification.

Acronym	Description
SNMP	Simple Network Management Protocol [2a][2b][2c]
MIB	Management Information Base, the standard data object and behavior description for SNMP
DevID	Device Identity, an IEEE 802.1AR Secure Device Identifier.
IDevID	An Initial DevID, assigned to the device by the OEM during production
LDevID	A Local DevID, assigned to the device by the user or administrator
OEM	Original Equipment Manufacturer

4. Conformance

4.1 Introduction

SNMP is an established network management protocol and method. While new methods and protocols are becoming more widely adopted, many networking equipment manufacturers and their customers have SNMP based management implemented. SNMP is therefore a good protocol for enabling the manufacturer, integrator, developer and customer community to gain experience with attestation as part of managing networking infrastructure.

4.2 SNMP Management - Normative

The SNMP Management Framework is described in IETF RFC documents, particularly Standard 58.

Managed objects are described via a Management Information Base or MIB, with MIB objects accessed through the Simple Network Management Protocol (SNMP) using the Object Identifiers defined in the MIB. Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information, version 2 (SMIv2).

This specification specifies a MIB module compliant with IETF standards as described in RFC 2578 and RFC 2579.

This specification is intended to interoperate with RFC 6933 (the Entity MIB) to allow attestation of devices, known as Composite Devices, that enclose multiple TPMs or multiple sub-devices, each with their own TPM. Such a composite device is not described explicitly in this specification. The MIB and operations specified here are structured to allow forms of composition as described in the entity MIB. Composite devices MUST implement the Entity MIB as described in RFC 6933 or later.

4.3 Security Considerations

4.3.1 Reconnaissance

The MIB provides for sending an SNMP notification when an attestation sequence is started. This is useful for identifying attestation performed with the intent of reconnaissance and should therefore be enabled in most deployments. The agent receiving the notification should monitor for use of attestation by unauthorized managers.

4.3.2 SNMP

SNMP by its nature is susceptible to several attacks. Mitigating SNMP attacks is outside the scope of this specification. For privacy and to provide authentication, use of SNMPv3 with AES encryption or SNMP over TLS are recommended.

The nature of TPM-based attestation data described here mitigates the risk of network spoofing or replays of SNMP data to a management entity or verifier.

4.3.3 Key Properties

Keys and certificates are specified elsewhere [1] and are outside the scope of this MIB. The user should be aware that attacks exist that use signing operations to break use of the same key for decryption. Further, a key that can be used for both signing and decryption cannot be a TPM restricted key—so it cannot be used to sign TPM2 internal data. For these reasons, a combined signing and decryption key is strongly discouraged.

To perform attestation with a TPM, an attestation key is required. An attestation key can signed certain data held internally by the TPM.

4.3.4 Legacy Compatibility

SHA-1 is obsolete and is included in the MIB only for compatibility with existing TPM 1.2 implementations that do not have SHA-2 capability. This MIB provides a SHA-1 option for `tcgTpmQuoteDigestSelector`, which is to be used only by those systems that have no SHA-2 or other hash available.

5. SNMP MIB Operation

5.1 MIB structure

The following MIB tree diagram provides a graphical overview of the MIB.

5.2 Example of Attestation with SNMP

SNMP operates on conceptual rows and columns, much like a row of a spreadsheet. More than one read or write operation may be required to retrieve or form one conceptual row. The MIB describes the row and column elements and their operations.

Devices with more than one TPM, known as Composite Devices, will require multiple attestations in order to assess the complete state of the device. It is expected that composite devices will implement the Entity MIB as needed to determine which TPM is to be selected for attestation.

The general attestation method is to first attest the main or current management interface and then use that interface for access to other devices within the system. As the internal interconnection topology is device specific, a detailed description of using of the Entity MIB is not described here.

A remote management entity may use this MIB to perform attestation using the following procedure:

1. Using the `tcgTpmSelector` value, read the `tcgTpmSelectorEntry`. This will provide information about the TPM that is required to interpret some of the responses to follow.
2. Check the local certificate cache to determine whether retrieving device certificates from the managed device is required. If certificate retrieval is required, use the `tcgTpmQuoteCertTable`. Use the columns `tcgTpmQuoteCertTpmSelector`, `tcgQuoteCertChainIndex`, `tcgQuoteCertType` and `tcgQuoteCertFragmentIndex` to read certificates from the remote device.
   a. The `tcgTpmQuoteCertTpmSelector` is the same value as the `tcgTpmSelector`.
   b. The `tcgQuoteCertType` selects which certificate chain is of interest. Permitted values are specified by the `CertType` textual convention.
   c. `tcgQuoteCertChainIndex` selects the certificate of interest within a particular chain.
   d. `tcgQuoteCertFragmentIndex` selects a fragment index (or “window” index) into the certificate to permit retrieval of certificates larger than the transport buffer (window) size.

   Iterate through the retrieval commands until all required certificates have been retrieved. Note that full retrieval normally needs to be performed only if the device is new on the network.
3. Before retrieving a signed quote from the TPM, a mutual exclusion lock must first be obtained. To get the mutual exclusion lock, perform a GET of the `tcgTpmQuoteLockTable`, specifying the TPM to be locked with the `tcgTpmQuoteLockTpmSelector`. The value returned in `tcgTpmQuoteTpmLockVal` provides a period of exclusion to perform a Quote operation.

   This lock will expire at the earlier of 1) timer expiration or 2) quote read completion.
4. To perform the TPM Quote, read the `tcgTpmQuoteEntry`. Each read request includes more index (selector) values to fill in the conceptual table row. Columns to be filled are the read-write data in the MIB row:
   - `tcgTpmQuoteTpmSelector`
   - `tcgTpmQuoteLockValue`

- tcgTpmQuoteCertSelector
- tcgTpmQuoteReqType
- tcgTpmQuoteNonce
- tcgTpmQuoteDigestSelector
- tcgTpmQuotePcrSelector
- tcgTpmQuotePCRDigestAlg

The first read operation may include as many of the read-write ("Index") column data values as will fit in a single PDU and must provide a RowStatus of Create-And-Wait. The SNMP agent will reply with RowStatus set to Not-ready. Once all read-write column data has been provided to the row, the agent will return the read-only data with a RowStatus of Active. If the read-only data will not fit into one PDU, subsets of the columns may be iteratively read until all columns have been retrieved.

After successfully reading the read-only column data, the SNMP manager writes a row-status of Not-in-service. This cancels the mutex lock and allows the SNMP agent to recover resources. If the quote operation does not complete within the timeout period, the SNMP agent will likewise set the RowStatus to Not-in-service and recover resources.

READ-WRITE Columns

a. The tcgTpmQuoteTpmSelector is as above.
b. The tcgQuoteLockValue was retrieved in step 3.
c. The tcgTpmQuoteCertSelector is used to select a key to sign the Quote. Use the value corresponding to the tcgTpmQuoteCertType desired.
d. The tcgTpmQuoteReqType is described in the MIB.
e. The tcgTpmQuoteNonce is a random value selected by the requestor and included in the signature as determined by the TPM specification. This nonce proves freshness of the response so care must be exercised in preventing nonce re-use or nonce predictability.
f. tcgTpmQuoteDigestSelector is the signature digest to be used. The permitted values differ by TPM version and described in the TpmDigestAlgo textual convention description.
g. The tcgTpmQuotePcrSelector tells the TPM what PCRs to include in the quote. The permitted values are described in the MIB.
h. RowStatus, which is used as described above.

READ-ONLY Columns

a. tcgTpmQuoteRespType is returned to inform the SNMP manager how to interpret the response.
b. tcgTpmQuoteQualifiedSigner is empty for TPM 1.2. For TPM 2, it's the TPMU_NAME qualified name of the key used for the quote signature.
c. tcgTpmQuoteClockInfo is empty for TPM 1.2. For TPM 2, the current TPMS_CLOCK_INFO structure is returned.
d. tcgTpmQuoteFirmwareVersion is the TPM firmware version.
e. tcgTpmQuote is the signed quote response for Quote (and Quote2) responses. This column is empty for AuditSessionQuote types.
f. tcgTpmQuoteLogFileLines returns the number of lines (entries) in a AuditSessionQuote log. For Quote and Quote2 responses, the value is 0.
g. tcgTpmQuotePCRDigest is an untrusted digest, included for diagnostic purposes.

5. Retrieve the event log by using the tcgTpmQuoteLogTable, using the following columns iterate though the log.
   - `tcgTpmQuoteCertTpmSelector`
   - `tcgTpmQuoteLogSelector`
   - `tcgTpmQuoteLogLineNumber`
   - `tcgTpmQuoteLogFragmentIndex`

   Note that by caching the log from one query to the next, the attestation verifier (SNMP Manager) can start with the previous `tcgTpmQuoteLogLineNumber`+1 as a check for whether there are new entries in the log to be retrieved.

   a. The `tcgTpmQuoteCertTpmSelector` is the same value as in step 3, above.
   b. The `tctTpmQuoteLogSelector` selects from the logs that may be available on the remote device.
   c. The `tcgTpmQuoteLogLineNumber` is the line of the log file to be retrieved.
   d. The one-based `tcgTpmQuoteLogFragmentIndex` selects a fragment index (or "window" index) into the selected log line.
   e. `tcgTpmQuoteLogLineBuf` is the log entry payload.
   f. `tcgTpmQuoteLogStatus` is RowStatus for the current row (line) entry.
6. Parse the log file and check recalculated PCR values against the returned Quote.

6. SNMP MIB – Normative

```
--
-- CERTTPM-MIB
-- MIB generated by MG-SOFT Visual MIB Builder
--

    CERTTPM-MIB DEFINITIONS ::= BEGIN

        IMPORTS
                InetAddressType, InetAddress
                        FROM INET-ADDRESS-MIB
                SnmpAdminString
                        FROM SNMP-FRAMEWORK-MIB
                OBJECT-GROUP, NOTIFICATION-GROUP
                        FROM SNMPv2-CONF
                internet, Integer32, Counter32, BITS, OBJECT-TYPE,
                MODULE-IDENTITY, NOTIFICATION-TYPE
                        FROM SNMPv2-SMI
                RowStatus, DisplayString, TEXTUAL-CONVENTION
                        FROM SNMPv2-TC;


        -- 1.3.6.1.4.1.21911.1.1
        tcgTpmQuoteMIB MODULE-IDENTITY
                LAST-UPDATED "201805070000Z"          -- May 07, 2018 at 00:00 GMT
                ORGANIZATION
                        "Trusted Computing Group,
                         Embedded Systems Workgroup,
                         Networking Equipment Subgroup"
                CONTACT-INFO
                        "Admin@trustedcomputinggroup.org
                         neteq-chair@trustedcomputinggroup.org"
                DESCRIPTION
                        "The MIB module for retrieving attestation information from
                         a device, including the boot integrity measurement log
                         and a TPM quote."
                ::= { tcgMibs 1 }



--
-- Textual conventions
--

        TpmDigestAlgo ::= TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
                        "The tcgTpmQuotePCRDigest algorithm.

                        Note that SHA-1 is obsolete and is included here only for
                         compatibility with existing TPM 1.2 implementations that
                         do not have SHA-2 capability.

                        Implementations that have SHA-2 capability MUST NOT
                         support SHA-1.

                        Digests and values listed match the TPM Algorithm
                        registry and are current as of January 18, 2018.”

                SYNTAX INTEGER
                        {
                        noDigest(1),
                        tpmDigestSHA1(2),
                        tpmDigestSHA2256(3),
                        tpmDigestSHA2384(4),
                        tpmDigestSHA2512(5),
                        tpmDigestSM3256(6),
```

```
                tpmDigestSHA3256(7),
                tpmDigestSHA3384(8),
                tpmDigestSHA3512(9)
                }

TpmQuoteClockInfo ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
                "Syntax for ClockInfo in a TPM Quote.
                TPM 1.2 will have size 0.
                TPM 2 will have size 17."
        SYNTAX INTEGER (0 | 17)

TpmQuoteFwVersion ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
                "TPM firmware version field."
        SYNTAX INTEGER (0 | 8)

TpmQuoteQualifiedSigner ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
                "Syntax for tcgTpmQuoteQualifiedSigner."
        SYNTAX INTEGER (0 | 66)

TcgTpmLogFile ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
                "Limit log file lines to positive Integer32 value."
        SYNTAX Integer32 (0..2147483647)

CertType ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
                "Key and certificate creation is outside the scope of this
                 MIB. Refer to the Security Considerations for this MIB
                 and to TCG DevID specifications for further information.

                 CertType encodes the way in which a configured
                 certificate will be used.

                 A leaf certificate does not have the intermediate or
                 root bits set.

                 Non-leaf certificates should indicate only intermediate
                 or root status.

                 The CertType for leaf certificate may have multiple bits
                 set in cases where the same certificate will be used in
                 multiple cases or situations.

                 Certificate chains are to be verified using
                 authority/subject key identifiers only. Refer to
                 RFC-5280 for required certificate path validation
                 algorithms.

                 A self-signed certificate cannot convey identity,
                 so may not have any other bit set."
        SYNTAX BITS
                {
                selfSigned(0),
                tpmEndorsement(1),
                initialDevID(2),
                initialAttestation(3),
                initialEncrypting(4),
                initialCombinedEncryptingSign(5),
                localDevID(6),
                localAttestation(7),
                localEncrypting(8),
                localCombinedEncryptingSign(9),
```

```
                        localSpecific(10),
                        intermediate(11),
                        root(12)
                        }

        QuoteReqType ::= TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
                        "The type of attestation requested.
                        TPM 1.2 always uses TpmQuoteReq (1). Response tctTpmQuoteRespType
                         will be either TpmQuote or TpmQuote2 depending on system
                         capability.
                        For TPM 2, either TpmQuoteReq or TpmAuditSessionQuoteReq(2)
                         may be used. QuoteReq requests a TPM2_Quote operation, while
                         AuditSessionQuoteReq requests an audit session to be used
                         as a quote."
                SYNTAX INTEGER
                        {
                        tpmQuoteReq(1),
                        tpmAuditSessionQuoteReq(2)
                        }

        QuoteRespType ::= TEXTUAL-CONVENTION
                STATUS current
                DESCRIPTION
                        "This indicates the quote type returned by quote/attestation
                         request."
                SYNTAX INTEGER
                        {
                        tpm12QuoteResp(1),
                        tpm12Quote2Resp(2),
                        tpm20QuoteResp(3),
                        tpm2AuditSessionQuoteResp(4)
                        }

        PhysicalIndex ::= TEXTUAL-CONVENTION
                DISPLAY-HINT
                        "d"
                STATUS current
                DESCRIPTION
                        "An arbitrary value that uniquely identifies the physical
                        entity.  The value should be a small positive integer.
                        Index values for different physical entities are not
                        necessarily contiguous."
                SYNTAX Integer32 (1..2147483647)


--
-- Node definitions
--

        -- 1.3.6.1.4
        private OBJECT IDENTIFIER ::= { internet 4 }


        -- 1.3.6.1.4.1
        enterprise OBJECT IDENTIFIER ::= { private 1 }


        -- 1.3.6.1.4.1.21911
        tcg OBJECT IDENTIFIER ::= { enterprise 21911 }


        -- 1.3.6.1.4.1.21911.1
        tcgMibs OBJECT IDENTIFIER ::= { tcg 1 }


        -- 1.3.6.1.4.1.21911.1.1
        tcgTpmQuoteMIB OBJECT IDENTIFIER ::= { tcgMibs 1 }
```

```
        -- 1.3.6.1.4.1.21911.1.1.1
        tcgQuoteMibVersions OBJECT IDENTIFIER ::= { tcgTpmQuoteMIB 1 }


        -- 1.3.6.1.4.1.21911.1.1.1.1
        tcgTpmQuoteMibVerBase OBJECT-TYPE
                SYNTAX Counter32
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                        "Number base (radix) for version reporting.
                        This object must remain the first object
                        in this OID tree."
                ::= { tcgQuoteMibVersions 1 }


        -- 1.3.6.1.4.1.21911.1.1.1.2
        tcgTpmQuoteMibVersion OBJECT-TYPE
                SYNTAX Integer32
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                        "The MIB version supported by the device.
                        The version is to be updated when items are added or
                         deprecated in this MIB. This object must remain the
                         second object in this OID tree."
                ::= { tcgQuoteMibVersions 2 }
-- MIB version reported in the base specified by tctTpmQuoteMibVerBase.
-- Version 1 of this MIB corresponds to the first TCG release.

        -- 1.3.6.1.4.1.21911.1.1.1.3
        tcgTpmQuoteMibGeneralVersionInfo OBJECT-TYPE
                SYNTAX SnmpAdminString (SIZE (0..160))
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                        "A text string identifying the device, including
                         model and software version.”
                ::= { tcgQuoteMibVersions 3 }


        -- 1.3.6.1.4.1.21911.1.1.2
        tcgTpmQuoteNotify OBJECT IDENTIFIER ::= { tcgTpmQuoteMIB 2 }


-- Notifications are an optional feature of this MIB.
-- As some uses of notifications may support security risk management,
-- control of notifications is not provided in this MIB.
        -- 1.3.6.1.4.1.21911.1.1.2.1
        tcgTpmQuoteNotificationData OBJECT IDENTIFIER ::= { tcgTpmQuoteNotify 1 }


        -- 1.3.6.1.4.1.21911.1.1.2.1.1
        tcgTpmQuoteLockHolderIpAddrType OBJECT-TYPE
                SYNTAX InetAddressType
                MAX-ACCESS accessible-for-notify
                STATUS current
                DESCRIPTION
                        "The Inet address type of an entity requesting a
                         TpmQuoteTable lock."
                ::= { tcgTpmQuoteNotificationData 1 }


        -- 1.3.6.1.4.1.21911.1.1.2.1.2
        tcgTpmQuoteLockHolderIpAddress OBJECT-TYPE
                SYNTAX InetAddress
                MAX-ACCESS read-write
                STATUS current
                DESCRIPTION
```

```
                "The Inet Address of an entity requesting a TpmQuoteTable
                 lock."
        ::= { tcgTpmQuoteNotificationData 2 }


-- 1.3.6.1.4.1.21911.1.1.2.2
tcgTpmQuoteNotifications OBJECT IDENTIFIER ::= { tcgTpmQuoteNotify 2 }


-- 1.3.6.1.4.1.21911.1.1.2.2.1
tcgTpmQuoteLockNotification NOTIFICATION-TYPE
        OBJECTS { tcgTpmQuoteLockHolderIpAddrType, tcgTpmQuoteLockHolderIpAddress }
        STATUS current
        DESCRIPTION
                "Notification sent when a new TPM quote lock row is created."
        ::= { tcgTpmQuoteNotifications 1 }


-- 1.3.6.1.4.1.21911.1.1.3
tcgTpmSelectors OBJECT IDENTIFIER ::= { tcgTpmQuoteMIB 3 }


-- 1.3.6.1.4.1.21911.1.1.3.1
tcgTpmSelectorTable OBJECT-TYPE
        SYNTAX SEQUENCE OF TcgTpmSelectorEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "This table lists all TPMs reachable by the SNMP agent.

                On composite platforms (where the entity MIB is implemented)
                 the tcgTpmSelector index returned will match entries in
                 entPhysicalIndex. This allows correlation of the attestations
                 provided by this interface to the physical devices
                 described in the entity MIB.

                The reported selectorIndex on each row is used when
                 accessing the tcgTpmQuoteCertTable, the tctTpmQuoteTable
                 and the tcgTpmQuoteLogTable.

                As stated in the Entity MIB (RFC 6933), physicalIndex
                 values are not necessarily contiguous.

                When the entity MIB is not implemented on the platform,
                 the first selector returned will always be the active
                 management CPU/TPM instance."
        ::= { tcgTpmSelectors 1 }


-- 1.3.6.1.4.1.21911.1.1.3.1.1
tcgTpmSelectorEntry OBJECT-TYPE
        SYNTAX TcgTpmSelectorEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "The details pertaining to a specific TPM."
        INDEX { tcgTpmSelector }
        ::= { tcgTpmSelectorTable 1 }


TcgTpmSelectorEntry ::=
        SEQUENCE {
                tcgTpmSelector
                        PhysicalIndex,
                tcgTpmClass
                        INTEGER,
                tcgTpmSpecRev
                        Integer32,
                tcgTpmSelectorDescription
                        SnmpAdminString,
                tcgTpmFirmwareVersion
```

```
                        OCTET STRING
         }

    -- 1.3.6.1.4.1.21911.1.1.3.1.1.1
    tcgTpmSelector OBJECT-TYPE
            SYNTAX PhysicalIndex
            MAX-ACCESS accessible-for-notify
            STATUS current
            DESCRIPTION
                    "This table lists all TPMs reachable by the SNMP agent.

                    On platforms where the entity MIB is implemented, the
                     tcgTpmSelector index returned will match entries in
                     entPhysicalIndex. This allows correlation of the
                     attestations provided by this interface to the
                     physical devices described in the entity MIB.

                    The reported selectorIndex on each row is used when
                     accessing the tcgTpmQuoteCertTable, the
                     tctTpmQuoteTable and the tcgTpmQuoteLogTable.

                    When the entity MIB is not implemented on the platform,
                     the first selector returned must always be the active
                     management CPU/TPM instance."
            REFERENCE
                    "Refer to entPhysicalIndex in the entity MIB (RFC-6933)."
            ::= { tcgTpmSelectorEntry 1 }


    -- 1.3.6.1.4.1.21911.1.1.3.1.1.2
    tcgTpmClass OBJECT-TYPE
            SYNTAX INTEGER
                    {
                    tpm12(1),
                    tpm20(2)
                    }
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
                    "TPM generation (i.e., family)"
            ::= { tcgTpmSelectorEntry 2 }


    -- 1.3.6.1.4.1.21911.1.1.3.1.1.3
    tcgTpmSpecRev OBJECT-TYPE
            SYNTAX Integer32
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
                    "When not available, a value of 0 must be returned."
            ::= { tcgTpmSelectorEntry 3 }


    -- 1.3.6.1.4.1.21911.1.1.3.1.1.4
    tcgTpmSelectorDescription OBJECT-TYPE
            SYNTAX SnmpAdminString (SIZE (0..128))
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
                    "Printable ASCII string describing the module or device
                     with the TPM. This string must begin with a
                     manufacturer-specific model number of the device
                     containing the TPM. Use of IDevID identity is
                     recommended."
            ::= { tcgTpmSelectorEntry 4 }


    -- 1.3.6.1.4.1.21911.1.1.3.1.1.5
    tcgTpmFirmwareVersion OBJECT-TYPE
            SYNTAX OCTET STRING (SIZE (8))
```

```
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "The firmwareVersion object is a 64 bit integer encoded in
                 network order specifying the TPM-vendor specific version
                 number.

                For a TPM 1.2 this field is the value reported by the TPM,
                 or 0 if there is no accessible value."
        ::= { tcgTpmSelectorEntry 5 }


-- 1.3.6.1.4.1.21911.1.1.4
tcgTpmQuoteLocks OBJECT IDENTIFIER ::= { tcgTpmQuoteMIB 4 }


-- 1.3.6.1.4.1.21911.1.1.4.1
tcgTpmQuoteLockTable OBJECT-TYPE
        SYNTAX SEQUENCE OF TcgTpmQuoteLockEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "This one row table creates a simple mutex for attestation."
        ::= { tcgTpmQuoteLocks 1 }


-- 1.3.6.1.4.1.21911.1.1.4.1.1
tcgTpmQuoteLockEntry OBJECT-TYPE
        SYNTAX TcgTpmQuoteLockEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "This table may have at most one active row at a time. The
                 row is created on read and exists until expiration of
                 the timeout value or completion of a tcgTpmQuoteTable
                 read sequence.

                A subsequent read while the lock is active must not return
                 the tcgTpmQuoteTpmLockVal currently in use. In such a
                 case, the operation may fail or return zero for the lock
                 value.”
        INDEX { tcgTpmQuoteLockTpmSelector }
        ::= { tcgTpmQuoteLockTable 1 }


TcgTpmQuoteLockEntry ::=
        SEQUENCE {
                tcgTpmQuoteLockTpmSelector
                        PhysicalIndex,
                tcgTpmQuoteTpmLockVal
                        Integer32,
                tcgTpmQuoteLockTimeout
                        Integer32
         }

-- 1.3.6.1.4.1.21911.1.1.4.1.1.1
tcgTpmQuoteLockTpmSelector OBJECT-TYPE
        SYNTAX PhysicalIndex
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "The TPM to access for Quote operation.
                Refer to tcgTpmSelectorTable for TpmSelector usage."
        ::= { tcgTpmQuoteLockEntry 1 }


-- 1.3.6.1.4.1.21911.1.1.4.1.1.2
tcgTpmQuoteTpmLockVal OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
```

```
        DESCRIPTION
                "Reading this value returns a random number (a non-negative
                 INTEGER32) to use when reading the tcgTpmQuoteTable and
                 also sets and starts a timer. The starting value of this
                 timer (in seconds) is returned in tcgTpmQuoteLockTimeout.
                 The caller will be allowed to use the random value as a
                 key to read the tcgTpmQuoteTable table until the read
                 has been completed or the timer expires.

                 tcgTpmQuoteLockNotification may optionally be sent in
                 response to reading this object."
        ::= { tcgTpmQuoteLockEntry 2 }


-- 1.3.6.1.4.1.21911.1.1.4.1.1.3
tcgTpmQuoteLockTimeout OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "This is the length of time, in seconds, before the
                 tcgTpmQuoteLockVal mutex expires. The value of the
                 timer is set by device firmware and is not
                 writable via SNMP."
        ::= { tcgTpmQuoteLockEntry 3 }


-- 1.3.6.1.4.1.21911.1.1.5
tcgTpmQuoteObjects OBJECT IDENTIFIER ::= { tcgTpmQuoteMIB 5 }


-- 1.3.6.1.4.1.21911.1.1.5.1
tcgTpmQuoteCertTable OBJECT-TYPE
        SYNTAX SEQUENCE OF TcgTpmQuoteCertEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "A table containing certificates. Certs must be parsable
                by the attestation verifier. All certs are transferred
                in DER (wire) format."
        ::= { tcgTpmQuoteObjects 1 }


-- 1.3.6.1.4.1.21911.1.1.5.1.1
tcgTpmQuoteCertEntry OBJECT-TYPE
        SYNTAX TcgTpmQuoteCertEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "A table for reading certificates from the managed device.
                All certs are transferred in DER format."
        INDEX { tcgTpmQuoteCertTpmSelector }
        ::= { tcgTpmQuoteCertTable 1 }


TcgTpmQuoteCertEntry ::=
        SEQUENCE {
                tcgTpmQuoteCertTpmSelector
                        PhysicalIndex,
                tcgTpmQuoteCertChainIndex
                        Integer32,
                tcgTpmQuoteCertType
                        CertType,
                tcgTpmQuoteCertFragmentIndex
                        Integer32,
                tcgTpmQuoteCertBuf
                        OCTET STRING,
                tcgTpmQuoteCertStatus
                        RowStatus
         }
```

```
        -- 1.3.6.1.4.1.21911.1.1.5.1.1.1
        tcgTpmQuoteCertTpmSelector OBJECT-TYPE
                SYNTAX PhysicalIndex
                MAX-ACCESS read-write
                STATUS current
                DESCRIPTION
                        "The value used is determined from reading the
                         tcgTpmSelectorTable."
                ::= { tcgTpmQuoteCertEntry 1 }


        -- 1.3.6.1.4.1.21911.1.1.5.1.1.2
        tcgTpmQuoteCertChainIndex OBJECT-TYPE
                SYNTAX Integer32 (1..16)
                MAX-ACCESS read-write
                STATUS current
                DESCRIPTION
                        "A device may have multiple certificates associated with each
                         TPM. This index selects from among configured certificate
                         chains. The CertType response indicates the application of
                         the cert chain returned. Chain indices are an uninterrupted
                         sequence. For each TPM and Chain Index, there may be zero
                         or more certificates available.

                        A value of 1 specifies the leaf certificate, with the value
                        increasing in the chain toward the root.”
                ::= { tcgTpmQuoteCertEntry 2 }
-- The number of accessible elements is determined by the value of the related CertChainCount value.

        -- 1.3.6.1.4.1.21911.1.1.5.1.1.3
        tcgTpmQuoteCertType OBJECT-TYPE
                SYNTAX CertType
                MAX-ACCESS read-write
                STATUS current
                DESCRIPTION
                        "An index for the type of certificate to be read.
                        Refer to the CertType textual convention in this MIB."
                ::= { tcgTpmQuoteCertEntry 3 }


        -- 1.3.6.1.4.1.21911.1.1.5.1.1.4
        tcgTpmQuoteCertFragmentIndex OBJECT-TYPE
                SYNTAX Integer32 (1..32)
                MAX-ACCESS read-write
                STATUS current
                DESCRIPTION
                        "Certificates may be larger in size than can be carried by
                         a single UDP packet. This interface divides each
                         certificate into a sequence of max 484-byte buffers. The
                         index (in 484 byte increments) of the certificate
                         fragment is specified in tcgQuoteCertFragmentIndex.”
                ::= { tcgTpmQuoteCertEntry 4 }


        -- 1.3.6.1.4.1.21911.1.1.5.1.1.5
        tcgTpmQuoteCertBuf OBJECT-TYPE
                SYNTAX OCTET STRING (SIZE (1..484))
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION
                        "A buffer containing (a portion of) a certificate."
                ::= { tcgTpmQuoteCertEntry 5 }


        -- 1.3.6.1.4.1.21911.1.1.5.1.1.6
        tcgTpmQuoteCertStatus OBJECT-TYPE
                SYNTAX RowStatus
                MAX-ACCESS read-write
                STATUS current
                DESCRIPTION
```

```
                "The row status for the cert row. To perform a cert read
                 operation:
                - write the tctTpmQuoteCertTpmSelector value, setting row
                  status to 'createAndWait'
                - write each of the read-write column variables to select the
                  desired certificate window parameters.
                - once writable columns are configured, set row status to
                  'active'.
                - read the row to get the read-only buffer value
                - iterate through the chain indeces, cert type and fragment
                  indeces as needed until required certificates have been
                  retrieved.
                - when complete, set row status to 'notInService'."
        ::= { tcgTpmQuoteCertEntry 6 }


-- 1.3.6.1.4.1.21911.1.1.5.2
tcgTpmQuoteTable OBJECT-TYPE
        SYNTAX SEQUENCE OF TcgTpmQuoteEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "A table for attestation."
        ::= { tcgTpmQuoteObjects 2 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1
tcgTpmQuoteEntry OBJECT-TYPE
        SYNTAX TcgTpmQuoteEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "An entry of the quote Table."
        INDEX { tcgTpmQuoteTpmSelector, tcgTpmQuoteLockValue }
        ::= { tcgTpmQuoteTable 1 }


TcgTpmQuoteEntry ::=
        SEQUENCE {
                tcgTpmQuoteTpmSelector
                        PhysicalIndex,
                tcgTpmQuoteLockValue
                        Integer32,
                tcgTpmQuoteCertSelector
                        Integer32,
                tcgTpmQuoteReqType
                        QuoteReqType,
                tcgTpmQuoteNonce
                        OCTET STRING,
                tcgTpmQuoteDigestSelector
                        TpmDigestAlgo,
                tcgTpmQuotePcrSelector
                        OCTET STRING,
                tcgTpmQuotePCRDigestAlg
                        Integer32,
                tcgTpmQuoteRespType
                        QuoteRespType,
                tcgTpmQuoteQualifiedSigner
                        TpmQuoteQualifiedSigner,
                tcgTpmQuoteClockInfo
                        TpmQuoteClockInfo,
                tcgTpmQuoteFirmwareVersion
                        TpmQuoteFwVersion,
                tcgTpmQuote
                        OCTET STRING,
                tcgTpmQuoteLogFileLines
                        TcgTpmLogFile,
                tcgTpmQuotePCRDigest
                        OCTET STRING,
                tcgTpmQuoteRowStatus
```

```
                        RowStatus
         }

-- 1.3.6.1.4.1.21911.1.1.5.2.1.1
tcgTpmQuoteTpmSelector OBJECT-TYPE
        SYNTAX PhysicalIndex
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "The TPM to access for Quote operation.
                A value of one (1) selects the TPM associated with the local
                 CPU. Any other selector value is determined by the management
                 entity after retrieving the tcgTpmSelectorTable."
        ::= { tcgTpmQuoteEntry 1 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1.2
tcgTpmQuoteLockValue OBJECT-TYPE
        SYNTAX Integer32 (1..2147483647)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "The value read from tcgTpmQuoteTableLock is used as a key
                 to allow access to the QuoteEntry row. The value read
                 from tcgTpmQuoteTableLock may be used once to read
                 tcgTpmQuoteEntry, which must occur before the
                 tcgTpmQuoteTableLock timeout expires.

                The SNMP agent receives data with an incorrect
                 tcgTpmQuoteLockValue, the data is to be discarded
                 without any effect on the current row.”
        ::= { tcgTpmQuoteEntry 2 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1.3
tcgTpmQuoteCertSelector OBJECT-TYPE
        SYNTAX Integer32 (1..16)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "This is the cert chain (as reported by
                 tcgTpmQuoteCertChainIndex) to use in performing
                 the TPM quote operation. This selection must
                 include a certificate with the
                 InitialAttestation, LocalAttestation or
                 LocalSpecific CertType."
        ::= { tcgTpmQuoteEntry 3 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1.4
tcgTpmQuoteReqType OBJECT-TYPE
        SYNTAX QuoteReqType
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "Type of attestation requested. Refer to QuoteReqType
                textual convention description.”
        ::= { tcgTpmQuoteEntry 4 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1.5
tcgTpmQuoteNonce OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE (20..64))
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "The nonce to use when requesting a Quote from the selected
                 TPM.
                 - For TPM 1.2, the nonce size is 160 bits.
                 - For TPM 2.0, the nonce size matches the size of the
                   digest to be used.”
```

```
        ::= { tcgTpmQuoteEntry 5 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.6
    tcgTpmQuoteDigestSelector OBJECT-TYPE
            SYNTAX TpmDigestAlgo
            MAX-ACCESS read-write
            STATUS current
            DESCRIPTION
                    "A selector for the tcgTpmQuotePCRDigest algorithm."
            ::= { tcgTpmQuoteEntry 6 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.7
    tcgTpmQuotePcrSelector OBJECT-TYPE
            SYNTAX OCTET STRING (SIZE (4))
            MAX-ACCESS read-write
            STATUS current
            DESCRIPTION
                    "This is a bitmask to select PCR registers in the TPM for
                     inclusion in the Quote response. Size is always 4 octets.
                     These 4 octets are right-aligned to the bitmask supplied
                     to a TPM, with PCR 0 represented with the right-most
                     (lowest order) bit. "
            REFERENCE
                    "TPM class is returned in the tcgTpmSelectorEntry table.

                    TPM 1.2 PCRs are selected as defined in TCG TPM 1.2 Part 2,
                    Section 8.1 (TPM_PCR_SELECTION)

                    TPM 2.0 PCRs are selected as defined in TCG TPM 2.0 Library
                    Specification, Part 2, Section 10.6.1 (PMS_PCR_SELECT)."
            ::= { tcgTpmQuoteEntry 7 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.8
    tcgTpmQuotePCRDigestAlg OBJECT-TYPE
            SYNTAX Integer32
            MAX-ACCESS read-write
            STATUS current
            DESCRIPTION
                    "This object is of TPM 2.0 type TPM_ALG_ID, contained within
                     a 32-bit TPM_ALGORITHM_ID, which defines the hash algorithm
                     used to compute the PCR digest.

                     For TPM 1.2, the value is set as appropriate for the
                     algorithm in use."
            REFERENCE
                    "Refer to TPM 2.0 Library Specification, Part 2, Section
                     6.3 for the definition of TPM_ALG_ID. TPM_ALGORITHM_ID
                     is specified in the TCG Algorithms Registry."
            ::= { tcgTpmQuoteEntry 8 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.9
    tcgTpmQuoteRespType OBJECT-TYPE
            SYNTAX QuoteRespType
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
                    "The TPM quote type returned.

                    When a Tpm2SessionQuote type is returned, the session audit
                     log must be read from the tcgTpmQuoteLogEntry table."
            REFERENCE
                    "Refer to tcgTpmQuote description."
            ::= { tcgTpmQuoteEntry 9 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.10
```

```
tcgTpmQuoteQualifiedSigner OBJECT-TYPE
        SYNTAX TpmQuoteQualifiedSigner
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "For a TPM 1.2 this field is empty.

                The qualifiedSigner object is of TPM 2.0 type TPMU_NAME and
                 designates the qualified name of the public key used for
                 the quote signature.

                The TPMU_NAME is a digest described in TPM 2. It consists of
                 the 16 bit TPM_ALG_ID encoded in network order of the name
                 hash algorithm used to generate the digest of the public
                 key, followed by the public key digest itself.”

        REFERENCE
                "TPM2B_NAME structure."
        ::= { tcgTpmQuoteEntry 10 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1.11
tcgTpmQuoteClockInfo OBJECT-TYPE
        SYNTAX TpmQuoteClockInfo
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "For a TPM 1.2 this field is zero length.

                The clockInfo object is of TPM 2.0 type TPMS_CLOCK_INFO and
                 consists of the subfields Clock, ResetCount, RestartCount
                 and Safe.”
        REFERENCE
                "TPMS_CLOCK_INFO is defined in TPM 2.0 Library Specification, Part 2,
                Section 10.11.1."
        ::= { tcgTpmQuoteEntry 11 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1.12
tcgTpmQuoteFirmwareVersion OBJECT-TYPE
        SYNTAX TpmQuoteFwVersion
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "The firmwareVersion object is a 64 bit integer encoded in
                 network order specifying the TPM-vendor specific version
                 number.

                For a TPM 1.2 this field is the value reported by the TPM,
                 or empty if there is no accessible value.

                This value is the same as that returned by
                 tcgTpmFirmwareVersion."
        ::= { tcgTpmQuoteEntry 12 }


-- 1.3.6.1.4.1.21911.1.1.5.2.1.13
tcgTpmQuote OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE (0..484))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "This object is retrieved in response to the requested
                 Quote/Attest operation.

                 Note: The returned data has a different structure depending
                 on the TPM class:

                  For TPM 1.2, the returned value is a TPM_QUOTE_INFO or a
                    TPM_QUOTE2_INFO structure.
```

```
                    For TPM 2, the returned value depends on the
                      TpmQuoteReqType. For a quote, the response is a
                      TPMS_ATTEST structure. Note that a TPM2_Quote does not
                      return the actual TPM PCR values.
                      For an AuditSessionQuote, this field is empty and the
                      response is retrieved using the TpmQuoteLogTable."
            REFERENCE
                    "TPM 1.2 Quote is defined in TPM 1.2 Main Part 3, Section
                     16.3. TPM 1.2 Quote2 is defined in TPM 1.2 Main Part 3,
                     Section 16.5.

                     An overview of TPM 2.0 PCR selection is provided in the
                     TPM 2.0 Library Specification, Section 17.5. Be aware of
                     the race condition described in section 17.6.2 of the
                     same document.

                    TPM2 Quote is defined in the TPM 2.0 Library
                     Specification, Section 18.4."
            ::= { tcgTpmQuoteEntry 13 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.14
    tcgTpmQuoteLogFileLines OBJECT-TYPE
            SYNTAX TcgTpmLogFile
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
                    "This object returns the log file length (in lines) at the
                     time the TPM quote was generated. The returned value may
                     be used in retrieving the tcgTpmQuoteLogEntry table."
            ::= { tcgTpmQuoteEntry 14 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.15
    tcgTpmQuotePCRDigest OBJECT-TYPE
            SYNTAX OCTET STRING (SIZE (0..64))
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
                    "This is an untrusted digest for diagnostic purposes.

                    The digest is computed by hashing the
                        tcgTpmNonce,
                        tcgTpmQuotePcrSelector
                        All selected PCR registers read from the TPM
                    using the algorithm selected by tcgTpmQuoteDigestSelector."
            ::= { tcgTpmQuoteEntry 15 }


    -- 1.3.6.1.4.1.21911.1.1.5.2.1.16
    tcgTpmQuoteRowStatus OBJECT-TYPE
            SYNTAX RowStatus
            MAX-ACCESS read-write
            STATUS current
            DESCRIPTION
                    "The row status for the quote. To perform a quote operation:
                    - write the tctTpmQuoteLockValue retrieved from the
                        tcgTpmQuoteLockTable and set row status to
                        'createAndWait'
                    - write each of the read-write column variables to set the
                      quote parameters.
                    - when writable columns are configured, set row status to
                      'active'.
                    - read the row to get the read-only values
                    - when complete, set row status to 'notInService'."
            ::= { tcgTpmQuoteEntry 16 }


    -- 1.3.6.1.4.1.21911.1.1.5.3
    tcgTpmQuoteLogTable OBJECT-TYPE
```

```
        SYNTAX SEQUENCE OF TcgTpmQuoteLogEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "A table to return boot event log entries."
        ::= { tcgTpmQuoteObjects 3 }


-- 1.3.6.1.4.1.21911.1.1.5.3.1
tcgTpmQuoteLogEntry OBJECT-TYPE
        SYNTAX TcgTpmQuoteLogEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "An entry of the QuoteLog table. Each row in the table
                 corresponds to one line of the selected quote event log."
        INDEX { tcgTpmQuoteCertTpmSelector, tcgTpmQuoteLogSelector, tcgTpmQuoteLogLineNumber,
                tcgTpmQuoteLogFragmentIndex }
        ::= { tcgTpmQuoteLogTable 1 }


TcgTpmQuoteLogEntry ::=
        SEQUENCE {
                tcgTpmQuoteLogTpmSelector
                        PhysicalIndex,
                tcgTpmQuoteLogSelector
                        INTEGER,
                tcgTpmQuoteLogLineNumber
                        TcgTpmLogFile,
                tcgTpmQuoteLogFragmentIndex
                        Integer32,
                tcgTpmQuoteLogLineBuf
                        OCTET STRING,
                tcgTpmQuoteLogStatus
                        RowStatus
         }

-- 1.3.6.1.4.1.21911.1.1.5.3.1.1
tcgTpmQuoteLogTpmSelector OBJECT-TYPE
        SYNTAX PhysicalIndex
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "A value of one (1) selects the TPM associated with the local
                 CPU. Any other selector value is determined from reading
                 the tcgTpmSelectorTable."
        ::= { tcgTpmQuoteLogEntry 1 }


-- 1.3.6.1.4.1.21911.1.1.5.3.1.2
tcgTpmQuoteLogSelector OBJECT-TYPE
        SYNTAX INTEGER
                {
                static(1),
                dynamic(2)
                }
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "Selects the static log or an implementation specific dynamic
                 log. PCRs related to a static log are reset only at boot.
                 PCRs related to a dynamic log may be reset more often, but
                 this behavior is platform and application specific."
        ::= { tcgTpmQuoteLogEntry 2 }


-- 1.3.6.1.4.1.21911.1.1.5.3.1.3
tcgTpmQuoteLogLineNumber OBJECT-TYPE
        SYNTAX TcgTpmLogFile
        MAX-ACCESS read-write
        STATUS current
```

```
        DESCRIPTION
                "Each row in the table is one log entry. This object uniquely
                 identifies the row to be returned."
        ::= { tcgTpmQuoteLogEntry 3 }


-- 1.3.6.1.4.1.21911.1.1.5.3.1.4
tcgTpmQuoteLogFragmentIndex OBJECT-TYPE
        SYNTAX Integer32 (1..6)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "Log entries may be larger in size than can be carried by a
                 single UDP packet. This interface divides each log entry
                 into a sequence of max 484-byte buffers. The 1-based
                 index of the buffer is specified in
                 tcgTpmQuoteLogFragmentIndex."
        ::= { tcgTpmQuoteLogEntry 4 }


-- 1.3.6.1.4.1.21911.1.1.5.3.1.5
tcgTpmQuoteLogLineBuf OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE (0..484))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
                "The returned event log entry."
        ::= { tcgTpmQuoteLogEntry 5 }


-- 1.3.6.1.4.1.21911.1.1.5.3.1.6
tcgTpmQuoteLogStatus OBJECT-TYPE
        SYNTAX RowStatus
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
                "Status of the conceptual row."
        ::= { tcgTpmQuoteLogEntry 6 }


-- 1.3.6.1.4.1.21911.1.1.6
tcgTpmQuoteNotificationGroup NOTIFICATION-GROUP
        NOTIFICATIONS { tcgTpmQuoteLockNotification }
        STATUS current
        DESCRIPTION
                "Notification group."
        ::= { tcgTpmQuoteMIB 6 }


-- 1.3.6.1.4.1.21911.1.1.7
tcgTpmSelectionGroup OBJECT-GROUP
        OBJECTS { tcgTpmSelector, tcgTpmSelectorDescription,
                tcgTpmQuoteDigestSelector, tcgTpmQuoteLogSelector,
                tcgTpmQuoteQualifiedSigner, tcgTpmQuotePCRDigestAlg,
                tcgTpmQuoteTpmLockVal, tcgTpmQuoteLockTpmSelector,
                tcgTpmQuoteTpmSelector, tcgTpmQuoteCertTpmSelector,
                tcgTpmQuotePcrSelector, tcgTpmQuoteLogTpmSelector }
        STATUS current
        DESCRIPTION
                "A group of objects used as table indices."
        ::= { tcgTpmQuoteMIB 7 }


-- 1.3.6.1.4.1.21911.1.1.8
tcgTpmQuoteObjectGroup OBJECT-GROUP
        OBJECTS { tcgTpmQuoteMibVersion, tcgTpmQuoteNonce, tcgTpmQuote,
                tcgTpmQuoteLogLineNumber, tcgTpmQuoteLogFragmentIndex,
                tcgTpmQuoteCertSelector, tcgTpmQuoteLockValue,
                tcgTpmQuoteCertTpmSelector, tcgTpmQuoteLogTpmSelector, tcgTpmQuoteTpmSelector,
                tcgTpmQuoteRespType, tcgTpmSpecRev, tcgTpmClass,
```

```
                        tcgTpmQuotePCRDigest, tcgTpmQuoteClockInfo,  tcgTpmFirmwareVersion,
                        tcgTpmQuoteFirmwareVersion, tcgTpmQuoteReqType, tcgTpmQuoteLockTimeout,
                        tcgTpmQuoteTpmLockVal, tcgTpmQuoteRowStatus, tcgTpmQuoteLockHolderIpAddrType,
                        tcgTpmQuoteLockHolderIpAddress, tcgTpmQuoteCertChainIndex, tcgTpmQuoteCertType,
                        tcgTpmQuoteLogLineBuf, tcgTpmQuoteLogStatus, tcgTpmQuotePcrSelector,
                        tcgTpmQuoteCertFragmentIndex, tcgTpmQuoteCertBuf,
                        tcgTpmQuoteCertStatus, tcgTpmQuoteLogFileLines }
                STATUS current
                DESCRIPTION
                        "The group of objects required to support boot log and TPM
                         Quote retrieval."
                ::= { tcgTpmQuoteMIB 8 }


        -- 1.3.6.1.4.1.21911.1.1.9
        tcgTpmQuoteMibVersionGroup OBJECT-GROUP
                OBJECTS { tcgTpmQuoteMibVerBase, tcgTpmQuoteMibVersion,
                        tcgTpmQuoteMibGeneralVersionInfo }
                STATUS current
                DESCRIPTION
                        "Objects to support MIB version."
                ::= { tcgTpmQuoteMIB 9 }


    END

--
-- CERTTPM-MIB
--
```