TCG Trusted Network Connect
TNC IF-T: Binding to TLS

Specification Version 1.0
Revision 16
18 May 2009
Published

Contact:
admin@trustedcomputinggroup.org

TCG Published

TCG

Copyright © 2005-2009 Trusted Computing Group, Incorporated.

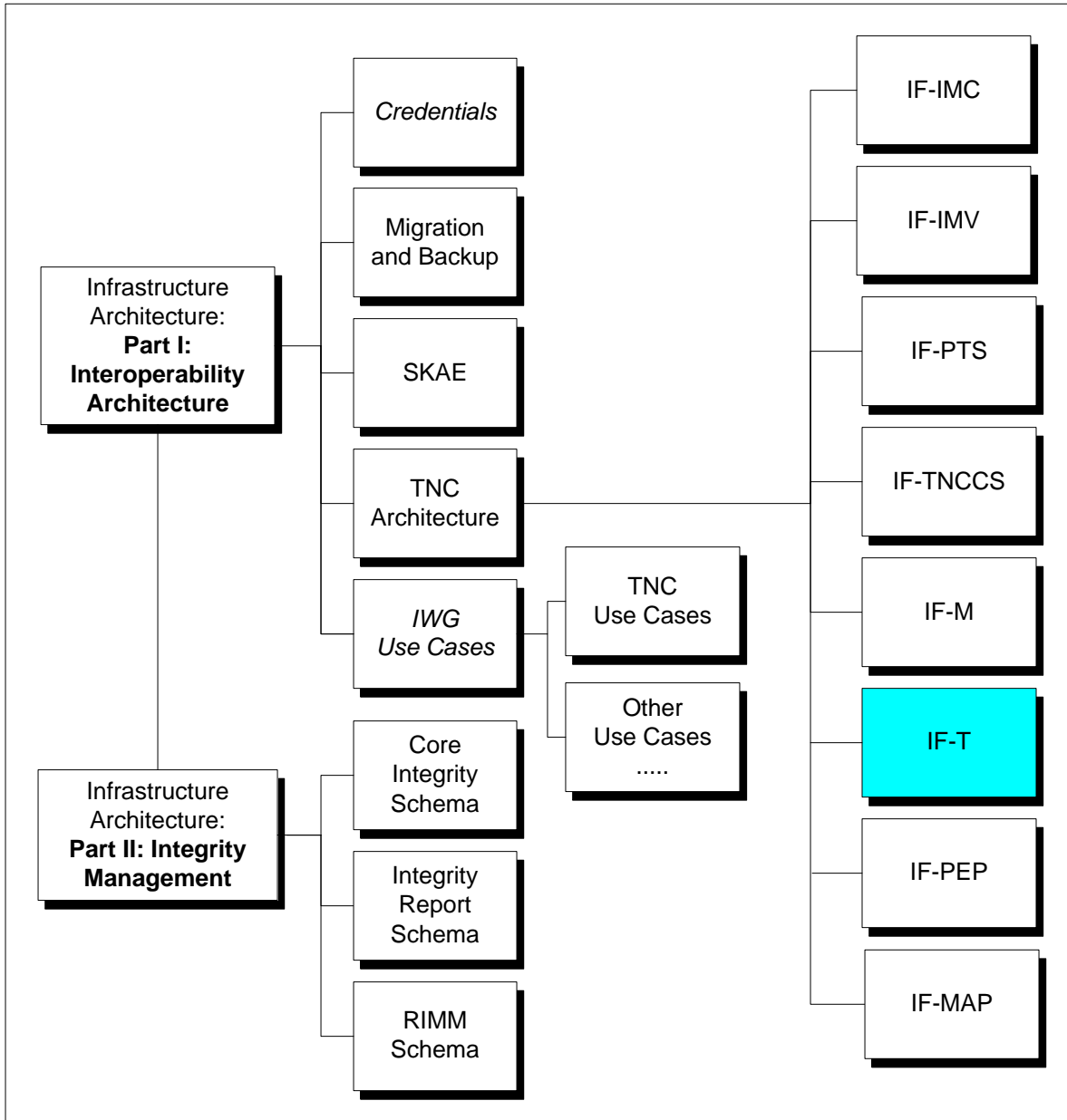**Disclaimers, Notices, and License Terms**

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

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

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

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

IWG TNC Document Roadmap

Credentials

Migration and Backup

Infrastructure Architecture:
Part I: Interoperability Architecture

SKAE

TNC Architecture

IF-IMC

IF-IMV

IF-PTS

IF-TNCCS

IF-M

IF-T

IF-PEP

IF-MAP

IWG Use Cases

TNC Use Cases

Other Use Cases .....

Infrastructure Architecture:
Part II: Integrity Management

Core Integrity Schema

Integrity Report Schema

RIMM Schema

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 TNC contributing to this document:

Name	Affiliation
Scott Kelly	Aruba Networks
Jeffery Dion	Boeing
Steven Venema	Boeing
Peter Wrobel	CESG
Mark Townsend	Enterasys
Sung Lee	Fujitsu Limited
Mauricio Sanchez	Hewlett-Packard
Ren Lanfang	Huawei
Dr. Jiwei Wei	Huawei
Han Yin	Huawei
Stuart Bailey	Infoblox
Ravi Sahita	Intel Corporation
Josh Howlett	JANET (UK)
Steve Hanna (TNC co-chair)	Juniper Networks
PJ Kirner	Juniper Networks
Lisa Lorenzin	Juniper Networks
Tom Price	Lumeta
Matt Webster	Lumeta
Paul Sangster (Editor, TNC co-chair)	Symantec
Brad Upson	University of New Hampshire InterOperability Lab
Lauren Giroux	US National Security Agency

Table of Contents

1   Scope and Audience

The Trusted Network Connect Work Group (TNC-WG) has defined an open solution architecture that enables network operators to enforce policies regarding the security state of endpoints in order to determine whether to grant access to a requested network infrastructure. This security assessment of each endpoint is performed using a set of asserted integrity measurements covering aspects of the operational environment of the endpoint. Part of the TNC architecture is IF-T, a standard protocol used to transport the TNC assessment exchanges leveraging the existing network connectivity. Because TNC enables assessment to occur during the process of joining a network and after the endpoint has been placed on the network, several bindings of IF-T will exist to address these different scenarios.

This document defines and specifies the IF-T protocol used when the endpoint is already on the network (has an IP address) and thus able to make use of higher layer protocols such as Transport Layer Security (TLS) [TLS12] to carry the assessment. Readers interested in the use of IF-T prior to joining the network (e.g. carrying EAP message over 802.1X) should refer to the TNC IF-T: Bindings to Tunneled EAP Method specification [IF-T-EAP].

Architects, designers, developers and technologists who wish to implement, use, or understand IF-T should read this document carefully. Before reading this document any further, the reader should review and understand the TNC architecture [TNC-ARCH].

2   Background

2.1   Purpose of IF-T

The IF-T protocol exists at the bottom of the TNC architecture protocol stack providing a transport service to carry the IF-TNCCS [IF-TNCCS] protocol over the available network. The TNC usage of IF-T enables assessments of endpoints as they are joining the network or after the endpoints are on the network. For scenarios when the endpoint is in the process of joining the network, the TNC assessment needs to be carried within the protocol used during the joining process. This protocol could be a layer two (link level) protocol, which needs to leverage an existing protocol such as 802.1 X that, allows for the exchange of EAP messages. This network join-time usage is the subject of the TNC IF-T Bindings to Tunneled EAP Methods specification. This specification focuses on the IF-T usage model where the endpoint is already present on the network and thus has an IP address assigned, so is reachable using TCP/IP by other systems.

This document describes and specifies the IF-T protocol using TLS [TLS12]. This binding of IF-T must at least provide the same level of service as other IF-T protocol bindings. Because the endpoint is on the network and able to leverage TCP/IP, this binding of the IF-T protocol may also provide enhanced capabilities (e.g. full duplex message exchange) to IF-TNCCS in addition to potentially higher quality of service (e.g. bandwidth).

2.2   Supported Use Cases

The following IF-T use cases must be supported:

1)   TNC Client initiated assessment or reassessment

   a)   TNC Client becomes aware of the need to perform an assessment

   b)   TNC Client uses TCP/IP to connect to the TNC Server over the network

   c)   TNC Server accepts the network connection

   d)   TNC Client and TNC Server exchange IF-T messages to set up a secure channel

   e)   TNC Client and TNC Server exchange IF-TNCCS messages to perform the assessment

   f)   TNC Client and TNC Server close the network connection

2)   TNC Server initiated assessment or reassessment

   a)   TNC Server becomes aware of the need to perform an assessment

   b)   TNC Server uses TCP/IP to connect to the TNC Client over the network

   c)   TNC Client accepts the network connection

   d)   TNC Client and TNC Server exchange IF-T messages to set up a secure channel

   e)   TNC Client and TNC Server exchange IF-TNCCS messages to perform the assessment

   f)   TNC Client and TNC Server close the network connection

3)   TNC Client establishes open connection for subsequent (TNC Client or TNC Server initiated) assessments

   a)   TNC Client joins a TCP/IP network (possibly including an assessment as per use case #1)

   b)   TNC Client uses TCP/IP to connect to the TNC Server over the network

    c)   TNC Server accepts the network connection

    d)   TNC Client and TNC Server exchange IF-T messages to set up a secure channel

    e)   TNC Client and TNC Server leave the network connection open until either decides that an assessment is necessary

    f)   TNC Client or TNC Server initiates an assessment

    g)   TNC Client and TNC Server exchange IF-TNCCS messages to perform the assessment

    h)   Upon completion of the assessment, the connection remains open for future use

4)   TNC Client and TNC Server send IF-TNCCS messages outside of an assessment. This use case may not impact IF-T unless IF-T is aware of IF-TNCCS state (start/end of an assessment).

    a)   TNC Client and TNC Server already have an L3 IF-T connection left open but no active assessment

    b)   TNC Client and TNC Server use this session to send IF-TNCCS messages without starting an assessment (e.g. to request a SAML assertion)

    c)   Upon completion of this exchange, the IF-T connection remains open for future use

5)   TNC Client and TNC Server use L3 and TLS IF-T connection to exchange non-TNC messages.

    a)   TNC Client and TNC Server have an open L3 IF-T connection, which may have been used for an earlier assessment

    b)   TNC Client and TNC Server use this session to send non-TNC messages (wrapped in special IF-T messages) without starting an assessment

    c)   Upon completion of this exchange, the IF-T connection remains open for future use

This allows a TNC assessment to be followed by and associated with an application layer exchange without needing to tie together two separate network connections

6)   Session reuse for reassessment

    a)   At the end of the IF-TNCCS message exchange (e.g. steps 1d, 2d and 3f above) the TNC Client and TNC Server elect to leave open the IF-T network connection

    b)   Either the TNC Client or TNC Server decides to perform a reassessment using the existing open IF-T network connection

    c)   TNC Client and TNC Server exchange IF-TNCCS messages to perform the assessment

7)   TNC Client dynamic discovery of TNC Server address prior to joining network

    a)   TNC Client and TNC Server exchange IF-TNCCS messages using a layer 2 IF-T protocol

    b)   At the conclusion of the layer 2 IF-T assessment, the TNC Client is provided the IP address of the TNC Server for future use while on the network.

    c)   TNC Client is given access to the network

TNC Client uses TCP/IP to connect to the TNC Server's IP address when an assessment is required or in advance of that time.

8) Security protected assessment

   a) Prior to the IF-TNCCS message exchange of the other use cases (e.g. steps 1d, 2d, 3f and 6c above), the TNC Client or TNC Server requests the authentication of the other party

      i) TNC Client may leverage a cryptographic credential or re-usable credential (password)

      ii) TNC Server must use a cryptographic credential to allow for strong server authentication

   b) TNC Client or TNC Server requests integrity and optionally confidentiality protection based upon byproducts of the authentication exchange.

   c) TNC Client and TNC Server negotiate security protections, algorithms and keys prior to performing the IF-TNCCS message exchange

2.3 Non-supported Use Cases

The following use cases are not supported by this specification:

- Use of IF-T Binding to TLS when TCP/IP connectivity can not be established

- Security protected assessment when no common trust anchor or cryptographic algorithms exist

- TNC Client dynamic discovery of TNC Server address after network connection (e.g. using DNS)

2.4 Requirements

Here are the requirements that the IF-T Binding to TLS must meet in order to successfully play its role in the TNC architecture and implement the use cases listed above.

- Meets the needs of the TNC architecture

  The IF-T Binding to TLS must support all the use cases described in the TNC architecture and this specification as they apply to transporting IF-TNCCS messages between the TNCC and TNCS.

- Security

  The IF-T Binding to TLS must be capable of protecting the integrity and confidentiality of the communications between the TNC Client and TNC Server. In order to protect against impersonation and active attacks (see security considerations section), the IF-T Binding to TLS must enable the TNC Client and TNC Server to strongly authenticate each other prior to the TNC assessment.

- Efficient

  The TNC architecture delays network access (or usage) until certain endpoint integrity checks have been performed. To minimize user frustration, it is essential to minimize delays and make communications using the IF-T Binding to TLS as rapid and efficient as possible.

Efficiency is also important for supporting lower powered, less capable endpoint devices or when dealing with low bandwidth network connections.

- Scalable

    The IF-T binding for TLS must make it easy for the TNC Server to support many hundreds or thousands of simultaneous TNC Client connections. An idle connection should impose as little overhead as possible. This is necessary for general scaling reasons but especially because one of the use cases calls for the TNC Client to establish an open connection that may be used for subsequent assessments and leave that connection open.

- Large Data Transport

    One of the benefits of the IF-T binding for TLS is that it should be able to carry much more data than the IF-T binding for Tunneled EAP Methods, which is limited by EAP's half-duplex nature, EAP authenticator timeouts, limits on EAP message size, etc. Also, one of the use cases above calls for the IF-T binding for TLS to be able to carry non-TNC (e.g. application layer) messages. This will result in even more data that needs to be carried.

- Reliable

    IF-T must provide reliable, in order, delivery of IF-TNCCS messages and be able to handle retransmission and fragmentation of messages if required by the underlying networking protocols.

- Full Duplex Permitted

    In order for the IF-T Binding to TLS to provide a consistent minimal level of service, every IF-T binding should allow for a half duplex dialog to be transported. However, the IF-T Binding to TLS must also allow for a full duplex exchange to occur. The half duplex support provides a minimal level of message delivery service that IF-TNCCS can rely upon across IF-T bindings while support for full duplex provides a path for more robust communications when the transport allows.

- Server or Client Initiated

    The IF-T Binding to TLS must be capable of being initiated by either the TNC Client or the TNC Server.

- Extensible

    The IF-T Binding to TLS will need to be expanded over time as new features are added to the TNC architecture and new use cases identified. The IF-T Binding to TLS must be capable of being extended to provide these additions in a way that is readily recognizable by the recipient.

- Agnostic

    The IF-T Binding to TLS must not require the interpretation of the contents of the IF-TNCCS protocol data elements as part of its operation. Changes to IF-TNCCS protocol must not require the replacement of the IF-T Binding to TLS.

2.5 Non-Requirements

Here are certain requirements that the IF-T Binding to TLS is not required to meet.

- Use Prior to Network Connectivity

  The IF-T Binding to TLS is not expected to be usable prior to the TNC Client possessing an
  IP address, routes and other information enabling it to have IP layer access to the network.
  For situations where the TNC Client is not yet present on the network, the IF-T binding to
  Tunneled EAP Methods should be used.

2.6   Assumptions

Here are the assumptions that this specification makes about the network connectivity available
to the TNC Client. This assumption differs from the expectations for only L2 connectivity used by
the prior IF-T Binding for Tunneled EAP methods.

- TCP/IP Connectivity

  Prior to the use of the IF-T Binding to TLS, the TNC Client and TNC Server are both able to
  communicate with each other over TCP/IP. This communication may be limited to the
  communication path between the TNC Client and TNC Server recognizing that the endpoint
  might only be able to reach a very small number of systems on the network during the
  assessment.

2.7   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 [KEYWORDS]. 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.

2.8   Network Communications Diagram Conventions

This specification includes diagrams illustrating the format and contents of network messages
exchanged between the Network Access Requestor (NAR) and Network Access Authority (NAA).
These diagrams depict the size of each field in bits. Implementations MUST send the bits in each
diagram as they are shown from left to right for each 32-bit quantity traversing the diagram from
top to bottom.   Multi-byte fields representing numeric values must be sent in network (big endian)
byte order. The values of each bit field (e.g. flags) are described referring to the position of the bit
within the field. These bit positions are numbered from the most significant bit through the least
significant bit, so a single byte field with only bit location 0 set has the value 0x80.

3   Network Connected Endpoint Assessments

This document specifies the IF-T binding for use when performing an assessment or reassessment after the endpoint has been admitted to the network and is capable of using TCP/IP to communicate with the TNC Server.   If the endpoint does not yet have TCP/IP layer access to the TNC Server (and vice versa), the endpoint should use the IF-T Binding to Tunneled EAP methods when performing an assessment.

Because the endpoint has TCP/IP access to the TNC Server (potentially on a restricted portion of the network), the TNC Client and TNC Server have the ability to establish (or re-use) a reliable TCP/IP connection in order to perform the assessment.   The TCP/IP connection enables the assessment to occur over a relatively high performance, reliable channel capable of supporting multiple roundtrip message exchanges in full duplex manner.   These connection properties are very different from what is available when the endpoint is initially joining the network (e.g. during an 802.1X based assessment), therefore the design described in this specification follows a different path to maximize the benefits of the connection properties.

3.1   Benefits

This binding of IF-T is normally able to offer to the TNC Client and TNC Server significantly higher quality of service and flexibility of operation than other bindings.   However, there may be some added risks when the endpoint is on the network prior to its initial assessment (if no admission time assessment is performed).   Because of these risks, the combined use of an EAP-based assessment during admission followed by reassessment using TCP/IP may be appropriate in many environments.

Some of the benefits to having a TCP/IP based transport during an assessment include:

- Full Duplex connectivity – can send multiple assessment messages prior to receiving a response including sending of asynchronous messages (e.g. alerts of posture changes)

- High Bandwidth – potentially much higher bandwidth than other transports (e.g. 802.1X) allowing more in-band data (e.g. remediation, verbose posture information)

- Reliability – IF-T messages sent will not be lost in transit (acknowledged by underlying protocol)

- In-order Delivery – IF-T messages can be sent knowing they won't be received prior to earlier messages

- Large Messages – ability to send very large IF-M messages without directly fragmenting them (underlying carrier protocol may introduce fragmentation)

- Bi-directional – TNC Client and TNC Server can initiate an (re)assessment

- Multiple Roundtrips – TNC Client and TNC Server can exchange numerous messages without fear of infrastructure timeouts.   However, the entire exchange should be kept as brief as possible in case the user has to wait for its completion.

In order to take full advantage of the above listed benefits, the IF-T binding in this specification does not re-use existing IF-T technologies (e.g. EAP and EAP-TNC).   However, this IF-T binding must still meet the same core set of IF-T requirements (e.g. security) in order for IF-TNCCS to be able to operate over both types of transports, but may provide additional or higher qualities of service.   See the Security Consideration section for details of how these requirements are met.

3.2   Securing the TCP/IP Session with TLS

All bindings of IF-T must be capable of providing strong authentication, integrity and confidentiality protection for the IF-TNCCS messages.   Rather than define a new protocol over TCP/IP to provide adequate protection, this specification requires the use of Transport Layer Security [TLS12] to secure the connection.   TLS was selected because it's a widely deployed

protocol with parallel protections to a number of the tunneled EAP methods, and it meets most of the security requirements (this specification will describe additional security protections offered in section 4.5). Therefore, the remainder of this specification will describe the use of IF-T on top of the TLS protocol.

4   IF-T Over TLS Protocol

This section specifies the IF-T transport protocol used on top of TLS. This protocol runs directly on top of TLS as an application. This means IF-T is encapsulated within the TLS Record Layer protocol using the standard ContentType for applications (application_data).   Because of the requirement to potentially share the TLS session with another protocol used between the TNC Client and TNC Server, this specification requires that all protocols sharing the TLS session (IF-T and any non-TNC protocols) include the type-length-value portion of the IF-T header to allow the recipient to identify the type of protocol (see section 4.3 for details).

4.1   TCP Port Usage

In order for an assessment initiator to establish a TCP connection to its peer, the initiator needs to know the TCP port number on which the recipient is listening for assessment requests. Note that for support of all of the above listed use cases, both TNC Client and TNC Server need to be capable of listening for requested assessments. Therefore, for version 1.0 of this specification, the TNC Client and TNC Server MUST each be capable of having its inbound TCP listening port configured. The TNC WG plans to request a well known TCP port number be reserved by the IANA to alleviate the need for this configuration following the issuance of this specification.

4.2   IF-T Message Flow

This section discusses the general flow of messages between the TNC Client's Network Access Requestor and the TNC Server's Network Access Authority in order to provide an assessment using the IF-T Binding to TLS. This section does not discuss the underlying message exchanges used by TCP and TLS, instead focusing on the IF-T messages.

4.2.1 Cause of an Assessment

Initially, the TNC Client or TNC Server will decide that an assessment is needed.   What stimulates the decision to perform an assessment is outside the scope of this specification, but some examples include:

- TNC Server becoming aware of suspicious behavior on an endpoint

- TNC Server receiving new policies requiring immediate action

- TNC Client noticing a change in local security posture

- TNC Client wishing to access a protected network or resource

Because either the TNC Client or TNC Server can trigger the establishment of the TLS session and initiate the assessment, this document will uses the terms "assessment initiator" and the "assessment responder". This nomenclature allows either TNC component to fill either of the IF-T roles.

4.2.2 Issues with Server Initiated TLS Sessions

The IF-T Binding to TLS allows for either the TNC Client or TNC Server to establish the TLS session. Allowing the TNC Server to establish the TLS connection means that TNC Clients will need to be listening for a connection request on a TCP port known by the TNC Server. In many deployments, the security policies (e.g. firewall) of an endpoint are designed to minimize the number of open inbound TCP/UDP ports that are available to the network to reduce the potential attack footprint. When the TNC Server creates a TLS session to the TNC Client, the TNC Client is effectively acting as the TLS server during the protocol exchange. This means the TNC Client would need to possess an X.509 certificate to protect the initial portion of the TLS handshake. In situations where the TNC Server initiates the creation of the TLS session, both the TNC Client and TNC Server MUST possess and use X.509 certificates to fully authenticate the session. For many deployments, provisioning X.509 certificates to all TNC Clients has scalability and cost issues; therefore, it is recommended that the TNC Client not listen for connection requests from

the TNC Server but instead establish and maintain a TLS session to the TNC Server proactively so either party can initiate an assessment using the preexisting TLS session as required.

Therefore, TNC Clients SHOULD be capable of establishing and holding open a TLS session with the TNC Server immediately after obtaining network access. TNC Client MAY allow for the TNC Server to establish a new TLS session when one does not already exist. Having an existing TLS session allows either party to initiate an assessment without requiring the TNC Client to be listening for new connection requests.

4.2.3 Establish or Re-Use TLS Session

If the assessment initiator already has TLS connectivity to the assessment responder, the initiator may re-use the session otherwise a new TLS session is required. Note that an existing TLS session between the NAR and NAA may be used to start an assessment regardless of which component originally established the session. If a TLS connection is re-used and another non-TNC message exchange is occurring, the assessment initiator may need to interpose its messages on the session. Therefore, every IF-T message MUST indicate what type of message (particular TNC specific or vendor specific) it contains so the recipient can handle it appropriately. This message type indication MUST distinguish IF-T assessment messages from other types of protocol messages. The NAR or NAA of the assessment responder is responsible for validating and removing the message type information prior to passing the messages up the protocol stack.

4.2.4 IF-T Message Exchange

The IF-T Binding to TLS message exchange occurs in three distinct phases:

- TLS Setup (includes TLS Handshake protocol)
- IF-T Pre-Negotiation
- IF-T Data Transport

The TLS Setup phase is responsible for the establishment of the TCP connection and the TLS protections for the IF-T messages. The TLS Setup phase normally starts with the establishment of a TCP connection between the NAR and NAA. The new connection triggers the TLS Handshake protocol to establish the cryptographic protections for the TLS session. The TLS Setup phase SHOULD NOT be repeated after the IF-T Data Transport phase has been reached unless a change of TLS cipher suite or keying material is required to properly protect the session.

The IF-T Pre-Negotiation phase is only performed at the start of the first assessment on a TLS session. During this phase, the NAR and NAA discover each others IF-T capabilities and establish a context that will apply to all future IF-T messages sent over the TLS session. The Pre-Negotiation phase MUST NOT be repeated after the session has entered the Data Transport phase. TNC assessment (IF-TNCCS) messages and other application messages should not be sent by the NAR or NAA prior to the completion of the IF-T Pre-Negotiation phase when the security protections for the session are in established and applied to the messages.

Finally the Data Transport phase allows the NAR and NAA to exchange IF-T messages under the protection of the TLS session and consistent with the capabilities established in earlier phases. The exchanged messages can be an IF-T protected assessment as described in this specification or other TNC Client/TNC Server exchanged messages.

4.2.4.1   TLS Setup Phase

After a new TCP connection is established between the NAR and NAA, a standard TLS exchange is performed to negotiate a common security context for protecting subsequent communications. As discussed in section 4.2.2, the TCP connection establishment and/or the TLS handshake protocol could be initiated by either the TNC Client or TNC Server. The most common situation would be for assessment initiator to trigger the creation of the TCP connection and TLS handshake so an assessment could begin when no session already exists. When the TNC

Server has initiated the TLS Setup, the TNC Server is acting as a TLS client and the TNC Client is the TLS server (accepting the inbound TLS session request). The expected normal case is that the TNC Client initiates this phase, so that the TNC Server is acting as the TLS server and therefore the bootstrapping of the security of the TLS session is using the TNC Server's certificate. Having the TNC Client initiate the TLS session avoids the need for the TNC Client to also possess a certificate.

During this phase the TLS session initiator (normally the TNC Client) contacts the listening port of the TLS session responder. The TLS session responder MUST possess a trustworthy X.509 certificate used to authenticate to the TLS initiator and used to bootstrap the security protections of the TLS session. The TLS initiator MAY also use an X.509 certificate to authenticate to the TLS responder providing for a bi-directional authentication of the TLS session.

TNC Client implementations of this specification integrated with a TCG trusted platform environment SHOULD be capable of using a client side X.509 certificate including the Subject Key Attestation Evidence (SKAE) extension [SKAE] for client authentication during the TLS handshake. The SKAE extension includes evidence that the private key associated with the public key found in the certificate is resident inside a TPM. The use of a TPM resident private key during the establishment of a TLS session provides a strong binding between a particular TPM on the TLS session initiator (TNC Client) and the TLS session being established. The TNC Server SHOULD process the certificate as usual and additionally performs a validation of the SKAE's evidence using the signing AIK private key. After the TLS session has been successfully created using a certificate containing the SKAE extension, the TNC Server SHOULD be capable of requesting an attestation using an Integrity Report [INTREPORT] from the PTS [IF-PTS] on the TNC Client leveraging the TPM resident key. The attestation would occur during the Data Transport phase using an IMV supporting the PTS information. The TNC Server SHOULD verify that the authentication credentials are associated with the same TPM as the one used for the PTS exchange. The strong cryptographic binding between the TNC Client's TLS identity and TPM resident key during the TLS handshake with the use of the TPM resident key during a subsequent attestation provides a countermeasure to MITM attack described in section 5. The active MITM is unable to both act as: the TNC Client (requesting network access) performing the TLS handshake using the certificate with the SKAE evidence and have access to TPM resident keys on another clean system. Therefore the TNC Server can detect when a different system is providing the attestation information than the system that performed the TLS handshake.

Due to deployment issues with issuing and distributing certificates to a potentially large number of TNC Clients, this specification allows the TNC Client to be authenticated during the Pre-Negotiation phase using other more cost effective methods. At the conclusion of a successful initial TLS Setup phase, the NAR and NAA have a protected session to exchange messages. This allows the protocol to transition to the IF-T Pre-Negotiation phase.

4.2.4.2   IF-T Pre-Negotiation Phase

Once a TLS session has been established between NAR and NAA, the assessment initiator sends a Version Request Message indicating its supported IF-T protocol version range. Next the assessment responder sends a Version Response Message which selects a protocol version from within the range offered. The assessment responder SHOULD select the preferred version offered if supported otherwise the highest version that it is able to support from the received Version Request Message. If the assessment responder is unable or unwilling to support any of the versions included in the Version Request Message, the responder SHOULD send a TNC_IFT_TLS_VERSION_NOT_SUPPORTED error message.

If no client side authentication has occurred during the TLS Setup phase, the NAA can authenticate the client using IF-T client authentication messages. If the NAA wishes to trigger a client authentication exchange, the NAA SHOULD send a Client Authentication Request message (see section 4.6 for details). The NAA MAY skip the Client Authentication Request exchange and instead start with the client authentication by sending a Client Authentication

Challenge message if it only supports one type of authentication. When the NAR receives the Client Authentication Request, the NAR responds with a Client Authentication Selection message indicating the method of authentication to be used. Upon selecting an appropriate authentication method, the NAA requests the client's identity and authenticator information using the IF-T Client Authentication Challenge Request message (see section 4.6.3 for details). The NAR responds with the requested information following the selected authentication scheme in a Client Authentication Response message. The NAA and NAR might exchange multiple roundtrips of client authentication messages in order to perform the authentication depending on the type of authentication selected. When the client authentication successfully completes, the IF-T session transitions into the Data Transport phase, where it will remain for the duration of the session.

4.2.4.3   Data Transport Phase

Once an assessment session is available to carry IF-TNCCS based assessments, either the NAA or NAR can start an assessment when provided an IF-TNCCS message for transmission. The assessment initiator envelopes the IF-TNCCS message in an IF-T message, assigning a message identifier to the message and sending it over the session. The assessment recipient validates the IF-T message and delivers the encapsulated IF-TNCCS message to its upstream component (TNC Client or TNC Server).

Most IF-T messages contain IF-TNCCS messages that request posture information or a response containing the requested information. The NAR and NAA may also exchange messages between them, such as an IF-T Error Message indicating that a problem occurred processing a message. During an assessment, the NAR and NAA merely encapsulate and exchange the IF-TNCCS messages and are unaware of the state of the assessment. The TLS binding of IF-T allows either party to send an IF-T message at any time reflecting the full duplex nature of the underlying TLS session. For example, an assessment initiator may send several IF-TNCCS messages prior to receiving any responses from the peer assessment responder. All implementations of the IF-T Binding to TLS MUST support full duplex IF-T message exchange. However, some IF-TNCCS protocols may not be able to make use of the full-duplex message exchange.

4.2.5 TLS Requirements

In order to ensure that strong security is always available for deployers and to improve interoperability, this section discusses some requirements on the underlying TLS transport used by IF-T. Implementations of IF-T Binding to TLS MUST support use of TLS 1.1 [TLS11] and SHOULD also include support for TLS 1.2 [TLS12].   For each TLS version supported, implementations of the IF-T Binding to TLS MUST at least support the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite. This cipher suite requires the server to provide a certificate that can be used during the key exchange. Implementations SHOULD NOT include the support for cipher suites that do not minimally offer NAA authentication, such as the anonymous Diffie-Hellman cipher suites (e.g. TLS_DH_anon_WITH_AES_128_CBC_SHA).

4.3   IF-T Message Format

This section describes the format and semantics of the IF-T Binding to TLS message. Every IF-T Binding to TLS compliant message MUST start with the IF-T header described in this section. The IF-T header provides a simple Type-Length-Value (TLV) based envelope around the IF-T message payload such as an IF-TNCCS message batch. Note that the Reserved and Message Identifier fields are technically part of the value portion of the TLV. However because these fields are required to be present in every IF-T message, they are described here as preceding the variant part (Message Value field) of the message.

Because this specification allows for other protocols to share the TLS session between the TNC Client and TNC Server, it is essential that those protocols be easily recognizable by the recipient. Therefore, all protocols sharing the TLS session with IF-T MUST start each protocol message with the initial five fields (between Reserved and Message Identifier inclusively) listed below. The

result is recipients can inspect the Message Type Vendor ID and Message Type and decide if and how they process the received message.

The following is the TLV-based protocol for IF-T:

```
                          1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Reserved    |              Message Type Vendor ID            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                          Message Type                          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                         Message Length                         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                        Message Identifier                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Message Value (e.g. IF-TNCCS Message) . . . .         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Header Field	Description
Reserved	This field MUST be set to 0 upon transmission and MUST be ignored by compliant IF-T message recipient implementations.
Message Type Vendor ID	This field indicates the owner of the name space associated with the Message Type. This is accomplished by specifying the 24 bit SMI Private Enterprise Number Vendor ID of the party who owns the Message Type name space. TCG standard TLVs defined in this specification MUST use the TCG SMI Private Enterprise Number value (0x005597) in this field.
Message Type	This field defines the type of the IF-T message within the scope of the specified vendor name space (Vendor ID) included in the Message Value field. The specific TNC standard values allowable in this field when the Vendor ID is the TCG SMI Private Enterprise Number value (0x005597) are defined in section 4.4. Recipients of a message containing a vendor id and message type that is unrecognized should respond with a TNC_IFT_TLS_TYPE_NOT_SUPPORTED error message.
Message Length	This field contains the length in octets of the entire IF-T message (including the entire header).
Message Identifier	This field contains a value that uniquely identifies the IF-T message on a per message sender (NAR or NAA) basis. This value can be copied into the body of a response message to indicate which message was received and caused the response. For example, this field is included in the IF-T Error Message so the recipient can determine which message sent caused the error. The Message Identifier MUST be a monotonically increasing counter starting at zero indicating the number of the messages the sender has transmitted over the TLS session. It is possible that a busy or long lived session might exceed $2^{32}-1$ messages sent, so the message sender MUST roll over to zero upon reaching the

	2^{32}nd message, thus restarting the increasing counter. During a rollover, it is feasible that the message recipient could be confused if it keeps track of every previously received Message Identifier, so recipients must be able to handle roll over situations without generating errors.
Message Value	The contents of this field vary depending on the particular Message Type being expressed. This field normally contains a IF-TNCCS message if the Message Type indicates IFT_TNCCS_20_BATCH, IFT_TNCCS_SOH_10_BATCH, or IFT_TNCCS_XML_10_BATCH.

4.4 IF-T Message Types

This section defines the TNC standard IF-T Message Types used to carry IF-T related and IF-TNCCS messages between the NAR and NAA. The following table summarizes the message type values that are used when the Vendor ID is set to the TCG SMI PEN (0x005597).

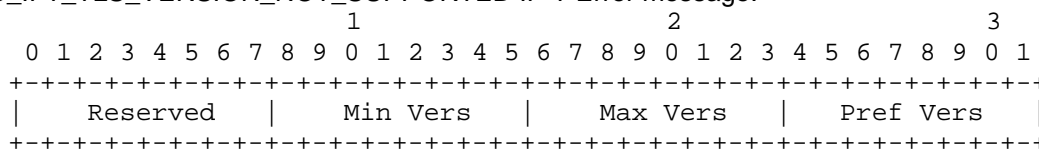| Message Type	Allowable Phase	Message Value Contents
0 (IFT_TYPE_EXPERIMENT)	Data Transport	Reserved for experimental use. This type will not offer interoperability but allows for experimentation.
1 (IFT_VERSION_REQUEST)	IF-T Pre-Negotiation	Contains a version negotiation request including the range of version supported by the sender.
2 (IFT_VERSION_RESPONSE)	IF-T Pre-Negotiation	Contains the IF-T protocol version selected by the responder.
3 (IFT_CLIENT_AUTH_REQUEST)	IF-T Pre-Negotiation	Contains the TNC Server's supported set of authentication methods and requests the TNC Client to select a supported and acceptable method. This message can be used to start an authentication of the TNC Client or in response to an attempt to access a protected resource requiring an authentication.
4 (IFT_CLIENT_AUTH_SELECTION)	IF-T Pre-Negotiation	Contains the TNC Client's selected client authentication method.
5 (IFT_CLIENT_AUTH_CHALLENGE)	IF-T Pre-Negotiation	Contains the client authentication challenge from the TNC Server.
6 (IFT_CLIENT_AUTH_RESPONSE)	IF-T Pre-Negotiation	Contains the client's identity and authenticator information.
7 (IFT_CLIENT_AUTH_SUCCESS)	IF-T Pre-Negotiation	Indicates that the client authentication performed has completed successfully so IF-T data messages may be sent.
8 (IFT_TNCCS_20_BATCH)	Data Transport	Contains an IF-TNCCS 2.0 message. For more information on IF-TNCCS

		messages see section 4 of the IF-TNCCS: Binding to TLV specification.
9 (IFT_TNCCS_SOH_10_BATCH)	Data Transport	Contains an IF-TNCCS 1.0 message. For more information on IF-TNCCS binding to SoH messages see the IF-TNCCS: Protocol Bindings for SoH specification [IF-TNCCS-SOH].
10 (IFT_TNCCS_XML_10_BATCH)	Data Transport	Contains an XML-based IF-TNCCS 1.x (1.0, 1.1 or 1.2) message. For more information on IF-TNCCS see the IF-TNCCS specification [IF-TNCCS].
11 (IFT_ERROR)	All	Contains an IF-T Error Message described in section 4.7.
12 (IFT_NON_TNC_DATA)	Data Transport	Contains non-TNC standard application data. This is for use by an application that is sharing the TLS session and does not wish to allocate a vendor defined message type to identify explicitly the data it is including. The sending application will need to have knowledge of how to place its data into the message value. Recipients need to have prior knowledge of the non-TNC data syntax and semantics included in the message.

4.5   IF-T Version Negotiation

This section describes the message format and semantics for the IF-T protocol version negotiation.   This message type allows the initiator of an IF-T session to trigger a version negotiation at the start of an assessment.   The IF-T session initiator MUST send a Version Request message as its first IF-T message and MUST NOT send any other IF-T messages on this connection until it receives a Version Response message or an Error message.   The IF-T session responder MUST complete the version negotiation (or cause an error) prior to sending or accepting reception of any additional messages.   After the successful completion of the version negotiation, both the NAA and NAR MUST only send messages compliant with the negotiated protocol version.   Subsequent assessments on the same session MUST use the negotiated version number and therefore SHOULD not send additional version negotiation messages.

4.5.1 Version Request Message

This message is sent at the start of the first assessment on an assessment session between the NAA and NAR. This message contains the sender's supported versions of the IF-T Binding to TLS protocol.   Recipients of this message MUST respond with a Version Response or an TNC_IFT_TLS_VERSION_NOT_SUPPORTED IF-T Error message.

```
                              1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Reserved   |    Min Vers   |    Max Vers   |    Pref Vers  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Header Field	Description
Reserved	This field MUST be set to 0 upon sending and MUST be ignored by compliant recipients.
Min Vers	This field contains the minimum version of the IF-T Binding to TLS protocol supported by the sender. This field MUST be set to 1 indicating support for the 1.0 version of this specification.
Max Vers	This field contains the maximum version of the IF-T Binding to TLS protocol supported by the sender. This field MUST be set to 1 indicating support for the 1.0 version of this specification.
Pref Vers	This field contains the sender's preferred version of the IF-T Binding to TLS protocol. This is a hint to the recipient that the sender would like this version selected if supported. The value of this field MUST fall within the range of Min Vers to Max Vers. This field MUST be set to 1 indicating support for the 1.0 version of this specification.

4.5.2 Version Response Message

This message is sent in response to receiving a Version Request Message at the start of a new assessment session.   If a recipient receives a Version Request after a successful version negotiation has occurred on the session, the recipient SHOULD send a TNC_IFT_TLS_INVALID_MESSAGE_ERROR error message and have TLS cleanly close the session.
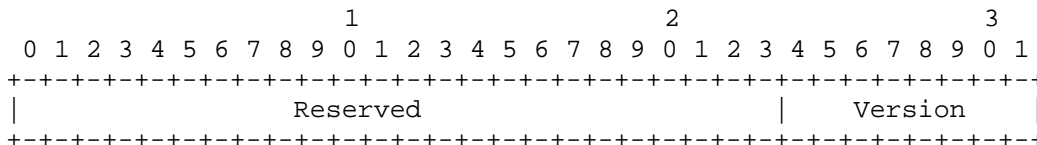
```
                          1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                  Reserved                     |     Version    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Header Field	Description
Reserved	This field MUST be set to 0 upon sending and MUST be ignored by compliant recipients.
Version	This field contains the version selected by the sender of this message. The version selected MUST be within the Min Vers to Max Vers inclusive range sent in the Version Request Message.

4.6 IF-T Client Authentication Message Exchange

This section includes a description of the message format and contents necessary to perform client authentication over IF-T Binding to TLS. The general model used for providing a client side authentication using IF-T messages over TLS is to have a simple TLV based authentication roughly equivalent to basic authentication for HTTP (as specified in RFC 2617) while also allowing for extensibility so stronger methods can be added in the future. Implementations compliant with the IF-T Binding to TLS specification MUST implement the Basic authentication type described in this section. Future specifications are expected to include additional types of

authentication. For example, it is expected that a widely used extensible authentication technology such as EAP [EAP] will be included in the future.

If a client authentication is required, the TNC Server MUST initiate the client authentication exchange by sending a Client Authentication Request message or a Client Authentication Challenge message. The Client Authentication Request message SHOULD be sent by the TNC Server when it is willing to authenticate the client using multiple alternative authentication methods. The Client Authentication Request message includes a prioritized list of the authentication methods that the TNC Server is willing to use with the TNC Client and allows the TNC Client to select one for use. When a TNC Server is only willing to accept a single use of a single authentication method, the TNC Server SHOULD optimistically start the authentication exchange by sending a Client Authentication Challenge in hopes that the TNC Client is willing and able to use the type of authentication. If the TNC Server requires client authentication but receives an IF-T message prior to client authentication successfully completing, the TNC Server should ignore the message and start the client authentication exchange (if it has not already done so).
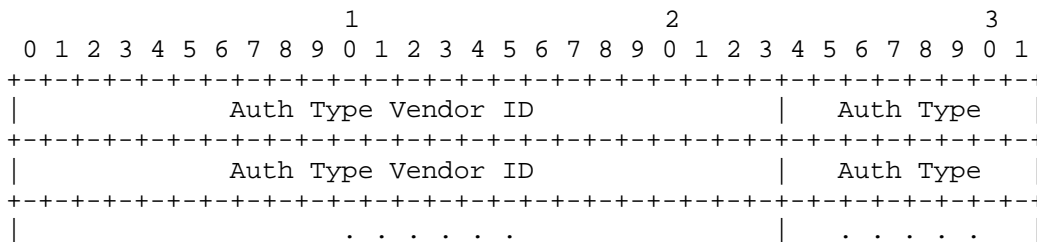
Upon reception of a Client Authentication Request, the TNC Client MUST send a Client Authentication Selection message that selects a single authentication method from the list in the Client Authentication Request message or send a TNC_IFT_TLS_AUTHENTICATION_ERROR error. When the TNC Server receives the Client Authentication Selection message, it MUST respond with a Client Authentication Challenge message containing the challenge information relevant to the selected type of authentication. Some authentication schemes might not require an initial server sent challenge so the Client Authentication Challenge message might contain minimal information and largely serve to start the authentication exchange. After the successful selection of an authentication method, the Client Authentication Request and Client Authentication Selection messages MUST NOT be used again on the session.

Now that an authentication method has been established, the client authentication involves a potentially multi-roundtrip message exchange until the TNC Server has confirmed the identity of the TNC Client. The number of roundtrip messages and the contents of each message depend on the type of authentication selected. The client authentication messages are described in the following sub-sections.

4.6.1 Client Authentication Request Message

This message is sent when the TNC Server has decided that a client authentication is required. This situation could occur following the initial establishment of the TLS session with the TNC Client or upon reception of a TNC Client message prior to successfully performing a required client authentication.

The following message shows the format of the Client Authentication Request message. Note that this message contains a list of Auth Type Vendor ID and associated Auth Type fields. The length of the TLV is used by the TNC Client to determine the number of authentication types offered in this message since each entry is 32 bits in length.

```
                      1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |              Auth Type Vendor ID              |   Auth Type   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |              Auth Type Vendor ID              |   Auth Type   |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   . . . . . .                 |   . . . . .   |
```

Header Field	Description

Auth Type Vendor ID	These fields indicate the owner of the name space associated with the following Auth Type field. Note that this field and the following Auth Type field will appear in pairs with one pair for every type of authentication being offered by the TNC Server being listed. The TNC Server may choose to skip sending the Client Authentication Request message if it only is willing to use a single form of client authentication, therefore eliminating the need for a negotiation and a roundtrip. The name space owner information is expressed as the 24 bit SMI Private Enterprise Number Vendor ID of the party who owns the Auth Type name space for the subsequent field. TCG standard TLVs defined in this specification MUST use the TCG SMI Private Enterprise Number value (0x005597) in this field.
Auth Type	These fields indicate a type of authentication that the TNC Server is willing to perform in order to authenticate the TNC Client's identity. The ordering of the authentication types in the list SHOULD be in the order of preference by the TNC Server. TNC Clients SHOULD process the list of authentication types in the order received and select the first type that is acceptable based on local policies.

4.6.2 Client Authentication Selection Message

This message is sent by the TNC Client in response to reception of a Client Authentication Request message. This message indicates the TNC Client's selection of an authentication method offered by the TNC Server. During the establishment of the TLS session, the TNC Client MAY authenticate to the TNC Server using a TLS defined client authentication method such as using client side certificates. If the TLS client authentication did not occur, the TNC Server SHOULD request the authentication of the TNC Client using the IF-T Client Authentication Request message.

The following message shows the format of the Client Authentication Selection message:

```
                      1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             Auth Type Vendor ID             |    Auth Type    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
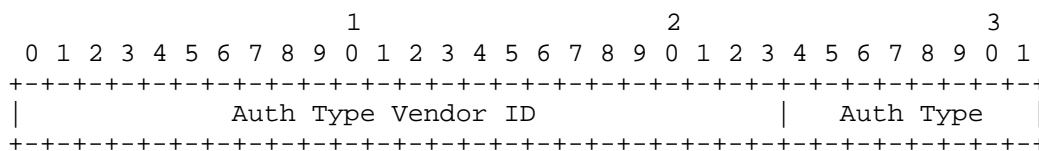
Header Field	Description
Auth Type Vendor ID	This field indicates the owner of the name space associated with the following Auth Type field that was selected by the TNC Client. The name space owner information is expressed as the 24 bit SMI Private Enterprise Number Vendor ID of the party who owns the Auth Type name space for the subsequent field. TCG standard TLVs defined in this specification MUST use the TCG SMI Private Enterprise Number value (0x005597) in this field.

	This field indicates a type of authentication that the TNC Client has selected from the list received from the TNC Server. The TNC Client MUST select one authentication type from the Client Authentication Request message from the TNC Server or send an TNC_IFT_TLS_AUTHENTICATION_ERROR error message. The TNC Client SHOULD process the list of authentication types received in order and select the first type that is acceptable based upon its policies.
Auth Type	

4.6.3 Client Authentication Challenge Message

This message is sent by the TNC Server to initiate the authentication of the TNC Client using the selected (in a Client Authentication Selection message) or TNC Server's only supported type of authentication. Based upon the type of authentication being performed, the contents of the Authentication Info field will vary. For the details of the Authentication Info field for the Basic Authentication type see section 4.6.3.1.

The following message shows the format of the Client Authentication Challenge message:

```
                      1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                Auth Type Vendor ID         |    Auth Type    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Challenge Information                     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             . . . . . .               |    . . . . .    |
```
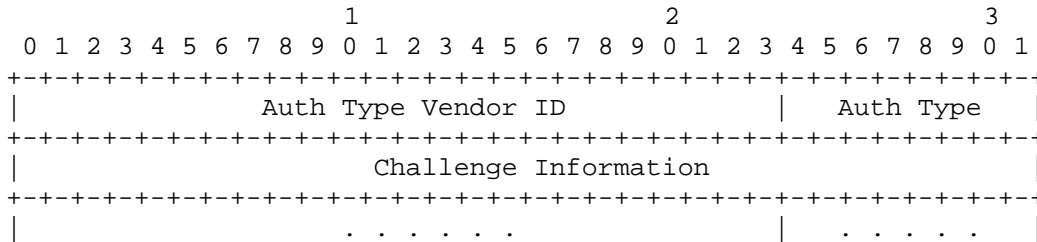
Header Field	Description
Auth Type Vendor ID	This field indicates the owner of the name space associated with the following Auth Type field that was selected by the TNC Client. The name space owner information is expressed as the 24 bit SMI Private Enterprise Number Vendor ID of the party who owns the Auth Type name space for the subsequent field. TCG standard TLVs defined in this specification MUST use the TCG SMI Private Enterprise Number value (0x005597) in this field.
Auth Type	This field indicates the type of authentication in use on the session. This field also indicates to the recipient the contents of the Challenge Information field (whose information varies based on authentication type and state).
Challenge Information	This field contains the authentication challenge in a format indicated by the type of authentication. The detailed format and semantics of this field for TCG specified authentication types are found in the following subsections.

4.6.3.1 Basic Authentication Challenge

This type of authentication is modeled on the HTTP basic authentication. This authentication involves the client sending a username and password (or passphrase) to the server for authentication. Note that the password will travel over the IF-T session without special protection, but it is afforded the full protections of TLS so passive attacks should be unable to steal these credentials.

For the Basic Authentication type of authentication, the Challenge Information field is empty. Basic authentication does not allow for the server to send information that alters the authentication response.

4.6.4 Client Authentication Response Message

This message is sent by the TNC Client to prove the identity of the client to the TNC Server. The format and contents of the Authentication Information vary depending on the type of authentication being performed and the state of the authentication exchange (e.g. when multi-roundtrip authentication protocols are used).

The following message shows the format of the Client Authentication Response message:

```
                          1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 Auth Type Vendor ID          |   Auth Type    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 Authentication Information                    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                . . . . . .                   |   . . . . .    |
```

Header Field	Description
Auth Type Vendor ID	This field indicates the owner of the name space associated with the following Auth Type field that was selected by the TNC Client. The name space owner information is expressed as the 24 bit SMI Private Enterprise Number Vendor ID of the party who owns the Auth Type name space for the subsequent field. TCG standard TLVs defined in this specification MUST use the TCG SMI Private Enterprise Number value (0x005597) in this field.
Auth Type	This field indicates the type of authentication in use on the session. This field also indicates to the recipient the contents of the Challenge Information field (whose information varies based on authentication type and state).
Authentication Information	This field contains the authentication information in a format indicated by the type of authentication. The detailed format and semantics of this field for TCG specified authentication types are found in the following subsections.

4.6.4.1 Auth Type Values

This section defines the TNC standard IF-T Auth Types used to identify the method of client authentication being used within a session between the NAR and NAA. The following table summarizes the Auth Type values used when the Auth Type Vendor ID is set to the TCG SMI PEN (0x005597).

Message Type	Definition
0 (IFT_AUTH_TYPE_RESERVED)	Reserved for experimental use. This type will not offer interoperability but allows for

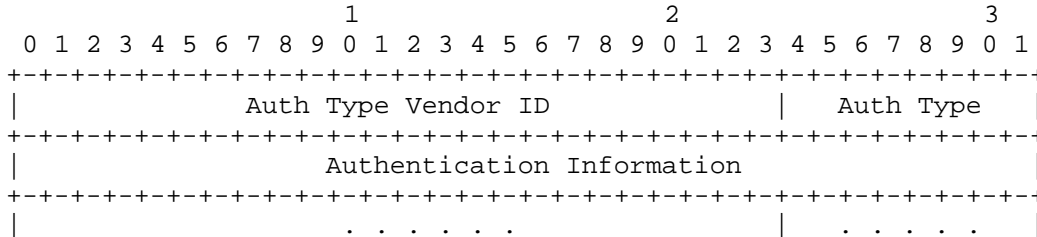|	
	experimentation.
1 (IFT_AUTH_TYPE_BASIC)	Indicates that the Authentication Information field contains a username and password as described in 4.6.4.2.

4.6.4.2 Basic Authentication Information

This type of authentication is modeled on the HTTP basic authentication. This authentication involves the TNC Client sending a username and password (or passphrase) to the TNC Server for authentication. The Authentication Information field will include the username and password for the TNC Client. The format and semantic are as follows:

```
                      1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             Auth Type Vendor ID          |    Auth Type     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |        Username Length        |            Username          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 . . . . . . . . . . . .                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                         Password                             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 . . . . . . . . . . . .                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Header Field	Description
Auth Type Vendor ID	This field indicates the owner of the name space associated with the following Auth Type field that was selected by the TNC Client. The name space owner information is expressed as the 24 bit SMI Private Enterprise Number Vendor ID of the party who owns the Auth Type name space for the subsequent field. TCG standard TLVs defined in this specification MUST use the TCG SMI Private Enterprise Number value (0x005597) in this field.
Auth Type	This field indicates the type of authentication in use on the session. This field also indicates to the recipient the contents of the Challenge Information field (whose information varies based on authentication type and state).
Username Length	This field indicates the length of the subsequent Username field. The Username field is variable length and is followed by the Password field which is also variable length so the recipient needs to be able to identify the end of the Username and the start of the password.
Username	This field contains a string containing the TNC Client's identity. The Username MUST be encoded as a UTF-8 string. NUL termination MUST NOT be employed.

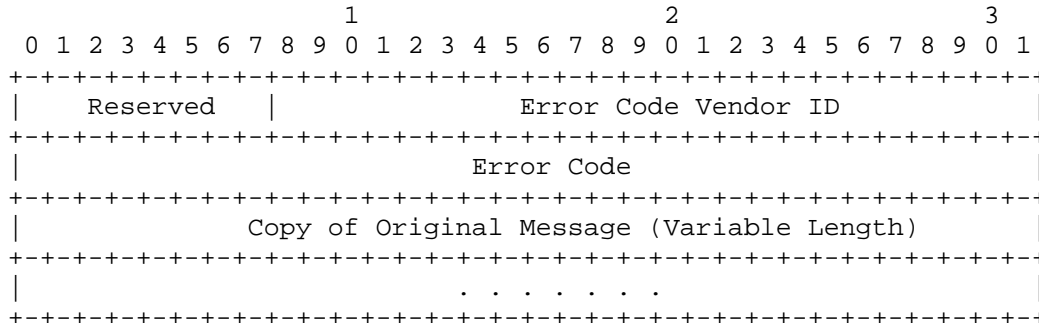|	This field contains a string containing the authenticator associated with the TNC Client's identity. For the Basic type of authentication, the Password field MUST include a UTF-8 encoded string. NUL termination MUST NOT be employed.
Password	

4.6.5 Client Authentication Successful Message

This message is sent by the TNC Server to indicate that it has successfully completed authentication of the TNC Client's identity and is now allowed to start sending assessment data messages. This message does not contain a Message Value field since the Message Type carries the only needed semantic (authentication was successful). The Client Authentication Successful message MUST be sent by the TNC Server at the completion of a successful authentication of the TNC Client to indicate that the initiator may now start sending TNC assessment messages.

4.7   IF-T Error Message

This section describes the format and contents of the IF-T Error Message sent by the NAR or NAA when it detects an IF-T level protocol error. Each error message contains an error code indicating the error that occurred, followed by a copy of the message that caused the error.

When an IF-T error is received, the recipient MUST NOT respond with an IF-T error because this could result in an infinite loop of error messages being sent. Instead, the recipient MAY log the error, modify its behavior to avoid future errors ignore the error, terminate the assessment, or take other action as appropriate (as long as it is consistent with the requirements of this specification).

The Message Value portion of an IF-T Error Message contains the following information:

```
                          1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Reserved    |            Error Code Vendor ID              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                          Error Code                           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |            Copy of Original Message (Variable Length)         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                       . . . . . .                             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Header Field	Description
Reserved	Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception.
Error Code Vendor ID	This field contains the IANA assigned SMI Private Enterprise Number for the vendor whose Error Code name space is being used in the attribute. For TCG standard Error Code values this field MUST be set to 0x005597. For other vendor-defined Error Code name spaces this field MUST be set to the SMI Private Enterprise Number of the vendor.

This field contains the error code. This error code exists within the scope of Error Code Vendor ID in this message that defined name space allowing for both vendor-defined and TCG standard name spaces. When the Error Code Vendor ID is set to the TCG Private Enterprise Number, the following table lists the supported TCG standard numeric error codes:

Value	Description
0	TNC_IFT_TLS_RESERVED_VALUE Reserved value indicates that the IF-T Error Message SHOULD be ignored by all recipients. This MAY be used for debugging purposes to allow a sender to see a copy of the message that was received while a receiver is operating on its contents.
1	TNC_IFT_TLS_MALFORMED_MESSAGE IF-T message unrecognized or unsupported. This error code SHOULD be sent when the basic sanity test fails. The sender of this error code MUST consider it a fatal error and abort the assessment.
2	TNC_IFT_TLS_VERSION_NOT_SUPPORTED This error SHOULD be sent when an assessment responder receives an IF-T Version Request message containing a range of version numbers outside the range the recipient is willing and able to support on the session. The sender of this error code MUST consider it a fatal error and close the TLS session after sending this IF-T message.
3	TNC_IFT_TLS_TYPE_NOT_SUPPORTED IF-T message type unknown or not supported. When an IF-T message recipient receives an IF-T message type that it does not support, it MUST send back this error, ignore the message and proceed. For example, this could occur if the sender used a Vendor ID for the Message Type that is not supported by the recipient.
4	TNC_IFT_TLS_AUTHENTICATION_FAILURE TNC Client has failed to authenticate to the TNC Server so session is to be terminated.
5	TNC_IFT_TLS_INVALID_MESSAGE_ERROR IF-T message received was invalid based on the protocol state. For example, this error would be sent if a recipient receives a message associated with the IF-T Pre-Negotiation (such as Version messages) after the protocol has reached the Data Transport phase. The sender of this error code MUST consider it a fatal error and close the TLS session after sending this IF-T message.
6	TNC_IFT_TLS_AUTHENTICATION_ERROR TNC Client is unable to support any of the offered types of authentication. The sender of this error code MUST consider it a fatal error and close the TLS session after

(Error Code)

Copy of Original Message	This variable length value contains a copy (up to 1024 bytes) of the original IF-T message that caused the error. If the original message is greater than 1024 bytes, only the initial 1024 bytes will be included in this field. This field is included so the error recipient can determine which message sent caused the error. In particular, the recipient can use the Message Identifier field from the Copy of Original Message to determine which one caused the error.

5 Security Considerations

This section discusses the countermeasures provided by the IF-T Binding to TLS protocol to the threats that each binding of IF-T transport protocol must face. Rather than replicate much of the security considerations from the IF-T Binding to Tunneled EAP Methods [IF-T-EAP], readers are directed to read section 5 of that specification to understand the threat environment and minimum security protections expected from IF-T.

Section 5.4.2 of the IF-T Binding to Tunneled EAP Methods establishes some common requirements that are to be addressed by all IF-T bindings. These 5 requirements are:

1. Cryptographic authentication of the NAA to the NAR

2. NAR authentication and TNC dialog protected by at least a cryptographic transport

3. Encryption of the message stream tied to at least the transport authentication

4. Cryptographic integrity protection of the message tied to at least the transport authentication

5. Protection against replay attack

The TLS binding of IF-T meets each of these requirements leveraging the cryptographic protections inherent in TLS. The following list discusses how each corresponding requirement is met by the protections provided by TLS:

1. All implementations of the IF-T Binding to TLS MUST support at least server (NAA) side certificate based authentication to the NAR using the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite. Deployers may choose to use other methods of authentication of the server, but all implementations will offer at least support for server certificate based authentication. When a TNC Client is capable of operating as the TLS server (accepting inbound IF-T TCP connections from the TNC Server), the TNC Client MUST also support the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite and have a certificate.

2. All implementations compliant with this specification MUST enable the NAR to authenticate using basic authentication over a cryptographically protected TLS record layer although they MAY allow this capability to be disabled by configuration. Implementations SHOULD also support cryptographic authentication mechanisms (e.g. client side certificates) to allow the NAR to authenticate during the TLS handshake prior to the protected TLS record layer. The TNC dialog (IF-TNCCS messages) is carried over the TLS record layer after a suitable cryptographic transport has been established. This allows for the entire TNC assessment to be protected from eavesdropping while on the network. Implementations of this specification targeting use on TCG trusted platforms SHOULD provide support for using client side TLS certificates containing the SKAE extension and allow for the use of the certificate with the trusted platform's trusted roots during attestation (e.g. signing an attestation Integrity Report using the SKAE extended certificate).

3. Because the TLS handshake protocol must support at least NAA side certificates, the resulting TLS record layer carrying the IF-T message stream will be protected by keys associated with the NAA authentication.

4. Again, the TLS handshake protocol will be capable of using a cryptographic authentication of the NAA using certificates. While under the protection of the NAA authentication exchange, keys are established to protect the integrity of each IF-T message sent using the TLS record layer.

5. There are a number of potential types of replay attack. Passive eavesdropping with later replay of observed information attacks are thwarted by the secrecy protection offered by the encrypting of the TLS record layer carrying the IF-T messages. Active replay attacks are addressed by the strong cryptographic authentication of the NAA by the NAR, thus

preventing rogue (untrusted) third parties from becoming a man in the middle intercepting and relaying messages. Similarly, the TLS record layer protects the NAR authentication from eavesdropping and replay.

Finally, section 5.4.5 of the IF-T Binding to Tunneled EAP Methods describes an active man in the middle attack where an adversary controlling a trusted NAA could trick a clean endpoint to provide compliant TPM based measurements. These measurements are recorded and replayed during an access-time assessment with a target network in order to appear compliant to gain access. As a countermeasure to this attack, the IF-T Binding to TLS allows for the use of client side certificates containing SKAE extensions during the authentication portion of the TLS handshake. The SKAE extension provides evidence that the private key associated with the public key contained in the certificate is housed and protected inside of the platform's TPM. The use of the certificate during the TLS handshake ensures that the TNC Client's identity and TPM resident private key are incorporated into the establishment of the TLS session keys. After the IF-T session has been established over TLS, when an assessment occurs the TNC Server SHOULD make use of an IMV supporting a TPM-based attestation (e.g. using the PTS). This assessment should leverage the TPM resident key to offer a signature over the assessment data and quote linking the reported measurements to the key known to be present on the TLS authenticated endpoint. These protections parallel those offered in the IF-T Binding to Tunneled EAP Methods, which also is able to leverage SKAE extensions to X.509 certificates.

6 Privacy Considerations

The role of IF-T is to act as a secure transport for IF-TNCCS and other higher layer protocols. As such, IF-T does not directly utilize personally identifiable information (PII) except when client authentication is enabled. When client authentication is being used, the TNC Client will be asked to disclose a local identifier (e.g. username) associated with the endpoint and an authenticator (e.g. password) to authenticate that identity. Because the identity and authenticator are potentially privacy sensitive information, the TNC Client MUST include a mechanism to restrict which TNC Server's will be sent this information. Similarly the TNC Client should provide an indication to the person being identified a request for their identity has been made in case they choose to opt out of the authentication to remain anonymous.

IF-T provides cryptographic peer authentication, message integrity and data secrecy to higher layer TNC protocols that may exchange data potentially including PII. These security services can be used to protect any PII involved in an assessment from passive and active attackers on the network. Endpoints sending potentially privacy sensitive information should ensure that the IF-T security protections (TLS cipher suites) negotiated for a TNC assessment of the endpoint are adequate to avoid interception and off-line attacks of any long term privacy sensitive information.

7 References

7.1 Normative References

[INTREPORT]   Trusted Computing Group, "TCG
                  Infrastructure Integrity Report
                  Schema Specification",
                  https://www.trustedcomputinggroup.or
                  g/specs/IWG/IntegrityReport_Schema_S
                  pecification_v1.0.pdf, November
                  2006.

[KEYWORDS]   S. Bradner, "Keywords for use in
                  RFCs to Indicate Requirement
                  Levels", **http://www.ietf.org/rfc/rfc
                  2119.txt**, IETF, March 1997.

[IF-PTS]   Trusted Computing Group, "TCG
                  Infrastructure Platform Trust
                  Services Specification (IF-PTS)",
                  https://www.trustedcomputinggroup.or
                  g/specs/IWG/IF-PTS_v1.0.pdf,
                  November 2006.

[SKAE]   Trusted Computing Group, "TCG
                  Infrastructure Subject Key
                  Attestation Evidence
                  Extension", **http://www.trustedcomput
                  inggroup.org/specs/IWG/IWG_SKAE_Exte
                  nsion_1-00.pdf**, June 2005.

[TLS11]   T. Dierks, E. Rescorla, "The
                  Transport Layer Security (TLS)
                  Protocol Version
                  1.1", **http://www.ietf.org/rfc/rfc434
                  6.txt**, IETF, April 2006.

[TLS12]   T. Dierks, E. Rescorla, "The
                  Transport Layer Security (TLS)
                  Protocol Version
                  1.2", **http://www.ietf.org/rfc/rfc524
                  6.txt**, IETF, August 2008.

[UTF8]   F. Yergeau, "UTF-8, a transformation
                  format of ISO
                  10646", **http://www.ietf.org/rfc/rfc3
                  629.txt**, IETF, November 2003.

7.2 Informative References

[EAP]   B. Aboba, "Extensible Authentication
                   Protocol", **http://www.ietf.org/rfc/r
                   fc3748.txt**, IETF, June 2004.

[TNC-ARCH]   Trusted Computing Group, "TNC
                   Architecture for Interoperability",
                   https://www.trustedcomputinggroup.or
                   g/specs/TNC/TNC_Architecture_v1_4_r2
                   .pdf, April 2009.

[IF-T-EAP]   Trusted Computing Group, "TNC IF-T:
                   Protocol bindings for Tunneled EAP
                   Methods",
                   https://www.trustedcomputinggroup.or
                   g/specs/TNC/TNC_IFT_v1_1_r10.pdf,
                   May 2007.

[IF-TNCCS]   Trusted Computing Group, "TNC IF-
                   TNCCS",
                   https://www.trustedcomputinggroup.or
                   g/specs/TNC/TNC_IF-
                   TNCCS_v1_1_r15.pdf, October 2006.

[IF-TNCCS-SOH]   Trusted Computing Group, "TNC IF-
                   TNCCS: Protocol Bindings for SoH",
                   https://www.trustedcomputinggroup.or
                   g/specs/TNC/IF-TNCCS-
                   SOH_v1.0_r8.pdf, May 2007.

[IF-IMC]   Trusted Computing Group, "TNC IF-
                   IMC",
                   https://www.trustedcomputinggroup.or
                   g/specs/TNC/TNC_IFIMC_v1_2_r8.pdf,
                   October 2006.

[IF-IMV]   Trusted Computing Group, "TNC IF-
                   IMV",
                   https://www.trustedcomputinggroup.or
                   g/specs/TNC/TNC_IFIMV_v1_2_r8.pdf,
                   October 2006.