



## **IF-T Binding to TLS Specification FAQ May 2009**

### **Q1. What is IF-T and how does it relate to TLS?**

A. IF-T is the “transport” layer protocol that is responsible for carrying the TNC’s protocol messages over the network. Because it’s the lowest TNC protocol layer, it needs to be able to operate over different network technologies so that TNC can perform assessments on different kinds of networks.

In 2006, TNC released an “IF-T Binding to Tunneled EAP Methods“ specification allowing for assessments of endpoints before having TCP/IP access. That IF-T binding leverages EAP, which is a common technology in 802.1X and IPsec’s Internet Key Exchange (IKE) protocol. The new IF-T Binding to TLS specification describes a method of running TNC assessment over a TLS session. This allows endpoints already on a TCP/IP network to be assessed.

### **Q2. When would a customer wish to use the IF-T Binding to TLS over the earlier IF-T Binding to Tunneled EAP Methods?**

A. The new TLS binding should be used when the endpoint is already present on a TCP/IP network and thus is able to protect an assessment with TLS security. The binding to tunneled EAP methods is intended for assessing of endpoints prior to being admitted on the network, so they do not have an IP address, routes or DNS information.

### **Q3. Why is IF-T Binding to TLS beneficial?**

A. The IF-T Binding to TLS is designed to support several new situations that are not well supported by the IF-T Binding to Tunneled EAP Methods:

- The IF-T Binding to TLS enables TNC assessments of endpoints that are already connected to a TCP/IP network. This differs from the earlier IF-T Binding to Tunneled EAP Methods that generally operated before the endpoint has access to the network (so lacks an IP address).
- The IF-T Binding to TLS also enables very verbose assessments of the endpoint since a TLS connection generally provides large bandwidth and support for many round trips. This could be beneficial if a TPM-based attestation is going to be used in addition to a TNC assessment.
- Finally, if the TNC Client and TNC Server are both able to initiate an assessment when either believes an event has occurred (e.g. suspicious behavior from endpoint) that warrants another assessment.

**Q4. Which versions of the IF-TNCCS protocol will operate over IF-T Binding to TLS?**

A. The IF-T Binding to TLS is a transport protocol that is agnostic of the higher layered protocol; therefore it can carry any of the IF-TNCCS protocol versions. In fact, it was designed to be able to share an existing TLS session with another non-TNC protocol. This was done so that a protocol running over TLS between the TNC Client and TNC Server could pause and allow a TNC assessment to occur. When the assessment completes, the non-TNC protocol can continue to use the TLS session.

**Q5. Can I use my existing TLS implementation?**

A. The IF-T Binding to TLS protocol is a protocol that operates on top of a standard TLS session. This means that existing TLS implementations can be used to carry the new IF-T protocol. No changes or extensions to the TLS library are required for this binding of IF-T to operate. However, application code must be modified or a shim installed.

**Q6. What vendors have implemented this specification?**

A. Several NAC vendors have similar proprietary protocols that operate over TLS. We expect to see increased adoption of the IF-T standard protocol after vendors and open source groups have time to review the specification. This protocol might be submitted to other standards groups to increase review and adoption.

**Q7. How does this specification relate to IETF NEA specifications?**

A. Both IF-T specifications align well with the IETF NEA architecture and requirements. We expect that these specifications will be considered for adoption by the NEA WG when the group standardizes the PT protocol later in 2009.

**Q8. Will this require a hardware or software upgrade?**

A. Generally speaking most NAC implementations are done in software, so should be field upgradable without replacing any equipment.

Contact: Anne Price, TCG market communications  
[anne@prworksonline.com](mailto:anne@prworksonline.com)  
1-602-840-6495