FAQ on Trusted Computing Group and the Internet Engineering Task Force

March 2010

Q. What is the Trusted Computing Group (TCG) doing with the Internet Engineering Task Force (IETF)?
A. Several years ago, TCG offered several TCG specifications to the IETF for standardization there. This month, IETF approved two new IETF standards based on those TCG standards. These TCG standards have been part of the TCG's Trusted Network Connect (TNC) architecture for years. Now they are also part of the IETF's long-standing series of Internet standards: the RFC series.

Also, OpenSEA Alliance announced its intention to add support for both protocols to the open source OpenSEA Xsupplicant.

Q. Which TCG documents were approved by IETF?
A. TCG's IF-TNCCS 2.0 and IF-M 1.0 were approved. IETF uses different names for these documents. In the IETF nomenclature, IF-TNCCS 2.0 is called PB-TNC and IF-M 1.0 is called PA-TNC. In any case, the IETF and TCG documents are equivalent and fully interoperable.

Q. Why is this important? Aren't people using the TNC standards already?
A. The TNC standards for Network Access Control (NAC) and network security are widely used. Dozens of products, thousands of customers, and millions of users use them every day to ensure that their networks are secure.

However, some vendors have held back from adopting the TNC standards because the TCG is an industry consortium and not an official standards body. Having the IETF's approval on these standards means that all parties have agreed on these standards as the proper way to do NAC on the Internet. Developers and customers can use the standards, knowing that they have been widely reviewed and agreed upon by the IETF's thousands of expert participants.

Q. How does this effort benefit customers?
A. IETF approval of these TNC standards will lead to more vendors implementing the standards. This will benefit customers in that products will become more widely interoperable and therefore easier to deploy and maintain. Over time, more and more products will have TNC support built in. Customers will be able to easily manage all of their network endpoints using these standards, leading to reduced costs and increased security.

Q. What does this mean for the TNC standards?
A. The TNC standards adopted by the IETF are just one small part of the overall TNC architecture, which also includes standards for other aspects of network security, such as clientless endpoint handling, hardware health checking, behavior monitoring, and information sharing among security devices. The TCG will continue to develop the TNC architecture and standards, adding features as needed.

Q. Why did the IETF decide to adopt the TNC standards?
A. As the IETF's Network Endpoint Assessment (NEA) Working Group defined requirements for NAC, it became apparent that the TNC standards met those requirements best. Therefore, it made sense for IETF to adopt these rather than developing separate, different standards.

Q. Which vendors have been involved in defining these standards?
A. Between the TCG TNC Work Group and the IETF NEA working group, a large number of vendors have been involved. It is not possible to list all of them. However, it is worth noting that the standards recently approved by the IETF and TCG had editors from Cisco, Intel, Juniper, Microsoft, and Symantec. This team worked together amicably to arrive at the resulting standards.

Q. What capabilities do these standards provide?
A. The fundamental capability provided by these standards is the ability to check the health (security posture) of an endpoint (network-connected device) and grant an appropriate level of network access. IF-TNCCS 2.0 is defines a standard protocol for health checking endpoints. IF-M 1.0 defines a standard format for the most basic health checks (e.g. anti-virus status).

Q. Is this the first time that TCG has worked with the IETF in this manner?
A. Yes, it is the first time that TCG standards have been accepted and approved by the IETF.

Q. When do you expect to see products that will use these new IETF standards?
A. The IETF plans to agree on standard NAC transport protocols by late 2010. Products generally begin to ship 6-12 months after standards are approved so one might expect to see products that implement the new standards some time in 2011.

Q. What if a customer needs to implement NAC before 2011?
A. Products that implement the TNC standards have been shipping since 2005. In fact, customers probably have products already deployed that include such support. Most enterprise-grade switches and wireless access points include support for the TNC enforcement standard, IF-PEP for RADIUS. And most modern versions of Windows include support for the TNC health checking standard, IF-TNCCS-SOH. So customers that need to implement NAC using open standards should use the TNC standards that have been in use for years.

Q. Will existing products based on earlier versions of the TNC standards work with future products based on the new versions of the TNC standards that the IETF has approved?
A. Due to the large installed base of products that implement the TNC standards, we expect that NAC vendors will include support for both versions of these standards in their NAC servers, thus providing a graceful client upgrade path.

Q. What's next for the IETF's work in the area of NAC industry standards?
A. The IETF NEA Working Group still has one important milestone. They must agree on standard NAC transport protocols. Once those are agreed upon, the IETF will have delivered standards for all the endpoint health-checking protocols.

Q. Will the TCG submit proposals for standard NAC transport protocols?
A. Yes. On January 4, 2010, the TCG submitted proposals for these protocols based on the TNC transport protocols: IF-T for Tunneled EAP Methods and IF-T for TLS. The first allows a health check before network access is granted. The second allows for health checking after network access has been granted. Together, they provide a complete and well-tested solution to the NAC transport protocol problem.

Q. IETF calls their documents RFCs, which is short for "Request for Comments". Does that mean that the documents are not yet standards?
A. No. The RFC name is historical, dating back more than 40 years. The RFC series includes all Internet Standards, as well as informational and experimental documents. The documents described here are on the IETF's standards track.

Contact:
Anne Price, TCG market communications
1-602-840-6495

anne@prworksonline.com