IEEE P802.11
Wireless LANs

|  |
| --- |
| Liaison from the IEEE 802.11 Working Group to ISO/IEC JTC1 SC6 and its National Body members in relation to claims about 802.1X/AE in N14399 and N14402 |
| Date: 2011-03-09 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document contains a proposed liaison from the IEEE 802.11 Working Group to ISO/IEC JTC1 SC6 and its National Body members.

The liaison is based on:

* ISO/IEC document ISO/IEC JTC1/SC6 N14399, which is a proposal for a NP for a standard that could replace IEEE 802.1X
* ISO/IEC document ISO/IEC JTC1/SC6 N14402, which is a proposal for a NP for a standard that could replace IEEE 802.1AE

The liaison will be considered by the IEEE 802.11 Working Group and IEEE 802 ExCom in March 2011.

### Liaison from the IEEE 802.11 Working Groupto ISO/IEC JTC1 SC6 and its National Body membersin relation to claims about 802.1X/AE in N14399 and N14402

At the last ISO/IEC JTC1/SC6 meeting in London, UK in September 2010, representatives of the Chinese National Body presented two documents proposing New Projects for the standardization of TePA-AC (N13399) and TLSec (N14402). It appears that these New Projects are being proposed to replace IEEE 802.1X and IEEE 802.1AE in some way based on perceived or claimed problems in these internationally recognized and widely used standards.

We have reviewed N13399 and N14402 and believe they contain significant misconceptions, misunderstandings and errors related to IEEE 802.1X and IEEE 802.1AE. Appendix A of this liaison contains a brief review of some of the claims about IEEE 802.1X and IEEE 802.1AE contained in N14402. We have not provided a separate review of N14399. We note as a caveat that neither contribution contains sufficient detail for us to provide a complete review. Appendix B of this liaison contains a limited review of the TLSec proposal in N14402. We have not yet undertaken a detailed review of TePA-AC. IEEE 802 is interested in hearing more details about TePA-AC and TLSec to help improve our understanding of these proposals.

We recommend that the members of ISO/IEC JTC1/SC6 engage with world recognized experts on IEEE 802.1X and IEEE 802.1AE and members of the IEEE 802.1 Working Group before approving the New Projects proposed by N13399 and N14402. The goal of any engagement would be ensure that SC6 has a proper and thorough understanding of IEEE 802.1X and IEEE 802.1AE before starting any project that might unnecessarily duplicate their functionality. We note that unnecessary duplication of standards is contrary to the explicit goals of IEEE, ISO/IEC and the WTO.

As a first step, we invite the proponents of these New Projects to present their work to the IEEE 802.1 Working Group. We also invite all interested members of ISO/IEC JTC1/SC6 to attend the presentation and participate in any subsequent discussions. We will provide minutes and a summary for any ISO/IEC JTC1/SC6 members who cannot attend the meeting in person.

We suggest the presentation and discussion occur at a IEEE 802.1 Working Group face to face meeting, which occurs approximately every two months. We propose the 17-22 July 2011 meeting in San Francisco as an appropriate venue because it is in a location relatively convenient to China, members of all IEEE 802 Working Groups will be in attendance and it is timely. IEEE 802 will assist with any visa applications for delegates from ISO/IEC JTC1/SC6 National Bodies.

Thank you for the opportunity to provide this liaison to ISO/IEC JTC1/SC6 and we look forward to interacting with the proponents of the New Projects and the members of ISO/IEC JTC1/SC6 in reviewing and possibly refining these proposals.

Yours sincerely,

Paul Nikolich
Chairman of IEEE 802 Working Group

# Appendix A:Review of claims in N14402 related to IEEE 802.1X/AE

### The claims in N14402 with respect to IEEE 802.1AE/X are inaccurate & misleading

N14402 is a presentation that documents a proposal for a New Project in ISO/IEC JTC1/SC6 to standardize a mechanism called TLSec, based on claimed inadequacies of IEEE 802.1AE and 802.1X. This appendix contains a high level assessment of the claims in N14402 related to IEEE 802.1AE and IEEE 802.1X, carried out by members of the IEEE 802.1 Working Group.

The overall conclusion of their assessment was:

*… comments on IEEE Std 802.1AE-2006/IEEE Std 802.1X-2010 are either inaccurate or could be misleading in a number of major respects particularly when presented those who are not familiar with the current state of the art of both bridging and security technology*

### 802.1X supports a flexible authentication framework

On page 11 of N14402 it is asserted that IEEE 802.1AE is incomplete. One of the reasons stated is that, “IEEE 802.1X-2010 doesn’t give a specific authentication mechanism."

It is certainly true that IEEE 802.1X-2010 doesn’t define a specific authentication mechanism. Instead, IEEE 802.1X supports the IETF defined EAP (Extensible Authentication Protocol) framework, which is extensively documented, along with multiple EAP methods (for authentication), in various IETF RFCs.

The use of a flexible EAP based framework enables:

* Users to select EAP methods and deployment options that meet the requirements imposed by the specific environment
* The introduction of new EAP methods as they are developed to meet new security threats and new environments

This approach was deliberately selected to meet the differing or changing requirements of diverse national interests and user/market segments in a variety of environments. If ISO/IEC JTC1/SC6 wishes to define a single authentication profile then one approach is to specify it in an International Standard Profile (ISP). IEEE 802 supports such an approach.

### 802.1X supports mutual authentication

On page 11 of N14402 it is asserted that IEEE 802.1AE is incomplete. One of the reasons stated is that, “Authentication in 802.1x is just between client and server.” The following statement, “The LAN switch doesn’t have an identity and is not authenticated”, then implies that 802.1X based solutions are subject to “man in the middle attacks”.

The claim that there is no mutual authentication in IEEE 802.1X based systems is untrue because the authentication server, switch and the client typically all participate in EAP based authentication exchanges.

A similar claim was made in the New Project proposal for WAPI with respect to the use of IEEE 802.1X in IEEE 802.11i based systems. The WAPI architecture appears to be similar to the architecture proposed in N14402. The claim in the New Project proposal for WAPI was shown to be incorrect in a liaison from IEEE 802 to ISO/IEC JTC1/SC6 in January 2011 (N14551). Interestingly, N14551 also demonstrated that WAPI does not actually directly mutually authenticate the AP and STA, and further noted that the WAPI authentication mechanism cannot be tailored to satisfy a variety of deployment and computation complexity tradeoffs required by realistic user environments.

The fact that IEEE 802.1X based systems do mutually authenticate authentication servers, switches and clients means the implication in N14402 that IEEE 802.1X based solutions are subject to “man in the middle attacks” is also untrue. A network administrator should require that any switch added to a network authenticate itself and 802.1X key management for 802.1AE works in such a way that switches can authenticate each other (neighbour to neighbour at an appropriate peer level) without loops of mutually dependency and can quickly recover an existing authentication for any link that goes down. The result is a network that is robust and secure and does not impose an excessive load on a central server during times of high change.

The issue of whether or not IEEE 802.1X provides mutual authentication is clearly an issue of disagreement. We believe that is will make an excellent topic for discussion between experts from IEEE 802.1 Working Group and ISO/IEC JTC1/SC6 at the proposed meeting.

### IEEE 802.1AE “hop by hop” encryption is an appropriate & scalable mechanism

On page 12 of N14402, it is suggested that 802.1AE is deficient because it uses “hop-by-hop” encryption. In particular, it is noted in N14402 that switches must decrypt and encrypt each packet, using different keys.

IEEE 802.1AE encryption is indeed "hop-by-hop", noting that one “hop” can span a single link or an entire network of provider bridges or provider backbone bridges (customer C-VLAN level for example).

However, a “hop-by-hop" architectures provides a more scalable and appropriate mechanism that the “end-to-end” alternative. “End-to-end” requires stations communicating with many other stations (or switches proxying for such stations) to maintain a separate cryptographic key and key schedule for each pair-wise communication. Ensuring rapid access to each key has a very large cost or performance impact for the end station, and requires special key sharing mechanisms for multicast throughout the entire network (not just on an access LAN). In contrast, IEEE 802.1AE requires only a single pair of keys per port. It is worth noting that the “hop-by-hop” architecture has not proved be a problem in real deployments today.

If “end-to-end” encryption is truly desired then the use of IPSEC (or other higher layer mechanisms) is strongly indicated. It is certainly undesirable to attempt to replace IPSEC with something that is just LAN specific. We note that a previous security standard, IEEE 802.10-1992, specified end to end encryption at the LAN link layer. It found no or very little adoption and was eventually withdrawn in 2004.

### IEEE 802.1AE meets known cost and performance goals

On page 12 of N14402, it is suggested that 802.1AE is deficient because it uses “hop-by-hop” encryption. In particular, it is noted in N14402 that IEEE 802.1AE is “high latency, high cost”.

It is difficult to respond to the claim that IEEE 802.1AE is “high latency, high cost” because N14402 does not specify any performance goals against which a statement can be evaluated. We request the authors of N14402 to provide customer validated cost and performance goals against which all solutions can be evaluated.

The cost vs latency performance balance is supported by the use of the GCM-AES cipher suite. GCM-AES operates in a pipeline mode whereby operations can start without knowing the data length. The level of latency is then a function of the degree of parallelism incorporated into the implementation.

Vendors are implementing and many users are deploying IEEE 802.1AE switches today, with an appropriate balance between cost and performance that appears to meet the needs of their customers.

### IEEE 802.1AE can interoperate with arbitrary switches & end stations

On page 12 of N14402, it is suggested that 802.1AE is deficient because it uses “hop-by-hop” encryption. In particular, it is noted in N14402 that IEEE 802.1AE suffers from “Flood is more terrible”.

A switch that is built to interoperate in a topology of neighbouring switches and end stations (some security capable, some not) must be capable of encrypting/decrypting to per-port level granularity. There is very little gained in terms of implementation cost by avoiding encrypt/decrypt at some times and not other times.

IEEE 802.1AE is designed to work with IEEE 802.1X to establish a secure topology of participating switches. The IEEE 802.1 Working Group would welcome the opportunity to explain this functionality.

### IEEE 802.1AE avoids propagating attacks to other switches

On page 12 of N14402, it is suggested that 802.1AE is deficient because it uses “hop-by-hop” encryption. In particular, it is noted in N14402 that IEEE 802.1AE suffers from “Flood is more terrible". "If the attacker sends a lot of frames with unknown MAC\_D, it can affect performance of the switch".

This point emphasizes how important it is that a switch verify the integrity/origin of a frame on reception (i.e. per port), rather than flooding it through the network and potentially sending that frame to a large number of other switches (some of which might in turn further flood the frame).

Reducing the encryption/decryption load on a switch by allowing it to propagate a problem to other switches in the network is generally counter productive. If the attacker sends frames with addresses that conflict with properly used addresses, then all traffic with those addresses can be affected in a bridged network. TLSec appears to suffer from this flaw.

# Appendix B:Review of TLSec proposal in N14402

### TLSec is a rearrangement of IEEE 802.11AE MACSec that does not address associated interworking/interoperability challenges

N14402 is a presentation that documents a proposal for a New Project in ISO/IEC JTC1/SC6 to standardize a mechanism called TLSec, based on claimed inadequacies of IEEE 802.1AE and 802.1X. This appendix contains a high level assessment of the TLSec mechanism.

The review in this appendix is based on an assessment of N14402 that was carried out by members of the IEEE 802.1 Working Group. It is limited in scope by the lack of detail available in N14402 related to TLSec.

Regardless of the limited scope of the assessment, it appears TLSec is just a slightly rearranged copy of IEEE 802.1AE MACsec that does not address associated interworking/interoperability challenges.

Interestingly, many of the pitfalls highlighted by this brief review of the TLSec proposal were discussed and avoided during the development of IEEE 802.1AE, IEEE 802.1X and IEEE 802.1Q. It does not seem productive to repeat these discussions given the existence of an existing internationally recognised standard that meets customer needs.

### TLSec appears to be a slightly rearranged copy of IEEE 802.1AE MACsec

TLSec appears to be (substantially) 802.1AE MACsec with communication over a VLAN instead of under all VLANs. In particular, it appears to be a re-arrangement of the interface stacks so that the C-VLAN tagging component is positioned underneath MACsec instead of above it.

In this respect it appears almost equivalent to the arrangement already described in IEEE 802.1AE clause 11.7 "MACsec in Provider Bridged Networks", but using the C-VLAN TAG (81-00) instead of the S-VLAN TAG. In this sense, TLSec is really just a copy of existing IEEE standards (even down to using terms/labels from IEEE 802.1AE and IEEE 802.1Q).

### TLSec does not address various interworking/interoperability challenges

N14402 presents no analysis of the interworking/interoperability challenges that follow from rearranging the interface stack for TLSec. For example:

* It is not clear whether the VLAN identifier (VID) is integrity protected (in which case it cannot be changed between source and destination) or not (in which case data/origin integrity is compromised).
* No analysis is presented of the desirability of having a network with insecure switches where traffic could be injected that would appear to peer with secure switches/clients (for example, how to manage such switches? what happens to secure multicast addressed to stations attached to them? and the myriad of issues that require a thorough understanding of the bridging standards etc.).

In contrast, IEEE 802.1AE clause 11.7 effectively already provides such an arrangement (traffic secured over a provider network) in a way that either avoids the interoperability and interworking issues or makes it clear how they should be addressed.