



IEEE 802

Local and Metropolitan Area Network Standards Committee

Date 30 MARCH 2017

DCN IEEE EC-17-0066-01-00EC

Source Paul Nikolich, Chairman IEEE 802 LAN/MAN Standards

To Dr. Hyun Kook Kahn Chair of ISO/IEC JTC1/SC6
kahng@korea.ac.kr
Mr. Yun-Jae Won Chair of ISO/IEC JTC1/SC6/WG1
yiwon@keti.re.kr

CC John D'Ambrosia IEEE 802 LMSC Recording Secretary
jdambrosia@ieee.org
Zhenhai Huang ISO/IEC JTC1/SC6 Mirror Committee, China
zhenhai.huang@iwncomm.com
Ms. Jooran Lee Secretary of SC6
jooran@ksa.or.kr
Andrew Myles Chair of IEEE 802 SC6 Standing Committee
amyles@cisco.com
Peter Yee Vice Chair IEEE 802 SC6 Standing Committee
peter@akayla.com
Konstantinos Karachalios Secretary, IEEE-SA Standards Board
Secretary, IEEE-SA Board of Governors
sasecretary@ieee.org

From Paul Nikolich Chairman, IEEE 802 Local and Metropolitan
Area Network Standards Committee
IEEE Fellow, p.nikolich@ieee.org

Subject Concerns relating to the proposed formation of a Security Ad Hoc within
JTC1/SC6

Approval Agreed at the IEEE 802 Vancouver 802 Plenary Session 17 March 2017

Dear Dr. Hyun Kook Kahng and Mr. Yun-Jae Won,

IEEE 802 has concerns relating to the proposed formation of a Security Ad Hoc within ISO/IEC JTC 1/SC 6. While IEEE 802 broadly supports the goal of improving security for SC 6-developed or approved standards, we believe that the Security Ad Hoc is not the best vehicle to accomplish this goal in relation to IEEE 802 standards submitted to SC 6 for possible ratification as ISO/IEC/IEEE 8802 standards under the PSDO agreement.

The presentation requesting the formation of the Security Ad Hoc noted that the China NB had presented detailed technical objections to the security mechanisms specified by ISO/IEC/IEEE 8802-1X. Those objections are summarized in 6N15613. The Switzerland NB representative at one time had some related concerns. IEEE 802 responded to those objections in 6N15658 and other later documents, showing that the alleged security flaws were not applicable to IEEE 802's use of the underlying security techniques and mechanisms.

IEEE 802 has requested, but not received, clarification on how our responses do not adequately address the alleged security flaws detailed in 6N15613. IEEE 802 has submitted similar requests for clarification for more than three years. Neither the China NB nor the Switzerland NB have provided additional evidence of the alleged security flaws in ISO/IEC/IEEE 8802-1X or have demonstrated any security flaws. Therefore, IEEE 802's response to each 60-day or FDIS ballot comment in the PSDO process that cites the alleged security flaws in ISO/IEC/IEEE 8802-1X has been to decline any changes to the proposed ISO/IEC/IEEE 8802 standard in question. This does not stem from any unwillingness on IEEE 802's part to modify the standards in response to properly justified comments originating from the PSDO process, but because it is impossible to address alleged security flaws for which there is no documented evidence.

IEEE 802 welcomes a substantive dialogue with SC6's security experts on these matters and has issued several invitations for SC6 NBs to participate in such discussions at IEEE 802 meetings (including one held in Beijing and, most recently, our just concluded meeting in Vancouver). With the exception of the Switzerland NB representative, who participated in a very productive discussion at the IEEE 802 meeting in Geneva in 2014, no other SC6 NBs have accepted our invitations. In contrast, IEEE 802 representatives have participated in such discussions at multiple SC6 meetings.

Given the China NB is the sole SC6 NB to submit comments as part of the PSDO process relating to alleged security flaws in ISO/IEC/IEEE 8802-1X, IEEE 802 believes it would be more productive for one or more representatives from the China NB to attend an IEEE 802 meeting to address their concerns about ISO/IEC/IEEE 8802-1X in person with the full range of IEEE 802 security experts. The goal of such a meeting would be to resolve this long-lasting impasse as quickly and efficiently as possible.

To summarize, while IEEE 802 supports the general goals of the proposed SC 6 Security Ad Hoc Group to improve security, IEEE 802 believes it will be more productive for a China NB representative to work directly with IEEE 802 security experts at an IEEE 802 meeting to resolve the China NB's concerns relating to ISO/IEC/IEEE 8802-1X. IEEE 802 reiterates its previous invitations for the China NB to attend an IEEE 802 plenary meeting, noting that IEEE 802's 9-14 July 2017 plenary meeting will be held in Berlin, Germany. This invitation is also extended to any SC6 NBs that would like to participate in or observe the discussions.

It is our sincere belief that direct dialogue will lead to resolution and IEEE 802 looks forward to working with the China NB and SC6 to resolve this long lasting open issue.

Yours sincerely,

/s/ Paul Nikolich

Paul Nikolich, Chairman of the IEEE 802 LMSC Executive Committee