P802.1Xbx

Submitter Email: tony@jeffree.co.uk
Type of Project: Amendment to IEEE Standard 802.1X-2010
PAR Request Date: 26-Jan-2012
PAR Approval Date:
PAR Expiration Date:
Status: Unapproved PAR, PAR for an Amendment to an existing IEEE Standard

1.1 Project Number: P802.1Xbx
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Local and metropolitan area networks--Port-Based Network Access Control Amendment: MAC Security Key Agreement protocol (MKA) extensions

3.1 Working Group: Higher Layer LAN Protocols Working Group (C/LM/WG802.1)
Contact Information for Working Group Chair
Name: Anthony Jeffree
Email Address: tony@jeffree.co.uk
Phone: +44-161-973-4278
Contact Information for Working Group Vice-Chair
Name: Paul Congdon
Email Address: paul.congdon@hp.com
Phone: 916-785-5753

3.2 Sponsoring Society and Committee: IEEE Computer Society/LAN/MAN Standards Committee (C/LM)
Contact Information for Sponsor Chair
Name: Paul Nikolich
Email Address: p.nikolich@ieee.org
Phone: 857.205.0050
Contact Information for Standards Representative
None

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 07/2013
4.3 Projected Completion Date for Submittal to RevCom: 10/2013

5.1 Approximate number of people expected to be actively involved in the development of this project: 10
5.2 Scope: This standard adds MACsec (Media Access Control security) Key Agreement protocol (MKA) data elements and procedures that provide additional security and manageability capabilities, including the ability to maintain secure communication while the operation of MKA is suspended, when used in conjunction with MACsec Cipher Suites that support Extended Packet Numbering.

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: This project will extend MKA to realize additional security and manageability capabilities made possible by the P802.1AEbt amendment that adds extended packet numbering Cipher Suites to IEEE Std 802.1AE-2006. These additional capabilities will include MKA data elements and procedures that allow secure connectivity association (CA) members to temporarily suspend MKA operation without causing protocol timeouts that would disrupt secure data transfer, thus allowing in-service control plane software upgrades.

5.5 Need for the Project: MKA already allows secure data transfer to continue without disruption as fresh keys are distributed and re-authentication and authorization takes place, potentially allowing any secured link or LAN to provide continuous connectivity for many years. One environmental factor likely to limit the longevity of this uninterrupted communication is the need to perform a control plane software upgrade. This fact has been recognized in the design of other networking protocols that include explicit support for continuing operation and state recovery when monitoring protocol actions need to be suspended and resumed. This project will allow such in-service upgrade capability when communication is being protected by 802.1AE MACsec in conjunction

with 802.1X. The IEEE Std 802.1AEbt extended packet numbering amendment will ensure that the interval between the need for fresh keys (even in very high speed operation) is greater than the time required for control plane upgrades, and this project is needed to realize the potential benefit.

5.6 Stakeholders for the Standard: Developers and users of networking equipment.

Intellectual Property
6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No
6.1.b. Is the Sponsor aware of possible registration activity related to this project?: No

---

7.1 Are there other standards or projects with a similar scope?: No
7.2 Joint Development
Is it the intent to develop this document jointly with another organization?: No

---

8.1 Additional Explanatory Notes (Item Number and Explanation):