P802.1AEbn

Submitter Email: tony@jeffree.co.uk
Type of Project: Amendment to IEEE Standard 802.1AE-2006
PAR Request Date: 07-Oct-2010
PAR Approval Date:
PAR Expiration Date:
Status: Unapproved PAR, PAR for an Amendment to an existing IEEE Standard

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

2.1 Title: Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security Amendment: Galois Counter Mode-Advanced Encryption Standard-256 (GCM-AES-256) Cipher Suite

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: 03/2013
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: 20
5.2 Scope: This standard specifies the optional use of the GCM-AES-256
Cipher Suite in addition to the existing Default Cipher Suite, GCM-AES-128.

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: This standard specifies the optional use of AES-256 for MAC
Security using GCM (Galois Counter Mode) and will update the 802.1AE-2006 references to support that specification.

5.5 Need for the Project: There is significant broad interest in the use of 256-bit AES data integrity and confidentiality with MAC Security. To promote
interoperability and ensure Cipher Suite quality, IEEE Standard 802.1AE requires that the Cipher suites used while claiming conformance are limited to those specified in the standard. This project will add the GCM-AES-256 Cipher Suite as an option.

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):