To: T10 SPC-4 Working Group
From: Matt Ball, M.V. Ball Technical Consulting, Inc.
Date: 2007-11-06
Subject: Proposed changes to Security algorithm codes table

Background

The table in SPC-4r11 entitled "Security algorithm codes" (Table 51 in r11) is currently using the NIST references 800-38C and 800-38D to describe the CCM and GCM algorithms. In practice, these encryption algorithms identify the modes within IEEE P1619.1 – not the modes described in the NIST standards.

This proposal is to change the CCM and GCM normative references to P1619.1, and also to add the XTS and CBC modes described in P1619.1 as new authenticated encryption modes.

Proposed Changes against SPC-4r11

{ Note: Additions in blue underline and deletions in ~~red strikethrough~~.}

Table 51 – Security algorithm codes

Code	Description	Reference
Encryption algorithms		
0001 000Ch	CBC-AES-256-HMAC-SHA-1	IEEE 1619.1
0001 0010h	~~AES-CCM with a 16 byte MAC~~CCM-128-AES-256	~~NIST SP 800-38C~~ IEEE 1619.1
0001 0014h	~~AES-GCM with a 16 byte MAC~~GCM-128-AES-256	~~NIST SP 800-38D~~ IEEE 1619.1
0001 0016h	XTS-AES-256-HMAC-SHA-512	IEEE 1619.1
...		