Industry Contribution for OmniAir WG Review / Recommendation for Standards / Specification, Testing, and Certification

Contribution Type: [Standard Change]
Specification Affected: [IEEE Std 1609.2-2025 Section 2 & 5.3.8]
Description Affected: [AES-SM4 Normative References]
Applicable OmniAir WG: [CyberSecurity]
WG Review: [Initial 2025-08-04]
WG Recommendation: [Posted on website until Standards Consideration]

Certification Test Spec Effect: [Incorporate into 1609.2]
Formatted for Public Posting: [Roebuck]
Document Identifier: [1609.2:2025 Note 2]

OmniAir Guidance Note GN-1609.2-2025-02: Normative references for AES, SM4

William Whyte – Qualcomm Inc

2026-04-24 d1 Original, 2026-08-13 d2 Formatting

Introduction

This Guidance Note provides guidance as to how OmniAir will interpret the subject standard (IEEE 1609.2-2025) with respect to material in that standard that is unclear or appears to be internally inconsistent.

The publication of this Guidance Note is not a commitment on the part of OmniAir to develop a test that will test the interpretation given in this Guidance Note. However, if such a test is developed, it will be consistent with the material given in this Guidance Note.

This Guidance Note applies to the indicated dated version of the subject standard. If a future version of the standard contains the same unclarity or inconsistency, a separate Guidance Note will be issued to apply to that standard. OmniAir members who will participate in the development of revisions of the subject standard may choose to draw attention to the unclarity or inconsistency identified in this Guidance Note, and to propose contributions to the revised standard to make it clear and consistent with the material given in this Guidance Note.

Technical Content: Issue

In 1609.2-2025, no normative reference in section 2 is provided in the text for AES, the Advanced Encryption Standard. A normative reference is provided for SM4, the Chinese national symmetric encryption algorithm, in 5.3.8, but it's wrong.

Technical Content: Resolution

Add the following line to the normative references in section 2:

ISO/IEC 18033-3:2010/AMD 1:2021 Information technology—Security techniques—Encryption algorithms—Part 3: Block ciphers—Amendment 1: SM4.

Replace the first paragraph of 5.3.8 with:

This standard supports two symmetric cryptographic algorithms: the Advanced Encryption Standard (AES) with 128-bit keys (specified in FIPS 197 and referred to below as “AES-128”) and SM4 (specified in ISO/IEC 18033-3:2010/AMD 1:2021).

Change History

2026-04-24 d1 (William Whyte) – Original

2026-08-13 d2 (Randy Roebuck) - Formatting