Homeland Security

Science and Technology

Office for Interoperability and Compatibility

Project 25 Compliance Assessment Bulletin

Project 25 Compliance Assessment Program

Encryption Requirements

P25-CAB-ENC_REQ

March 2017

Notice of Disclaimer and Limitation of Liability

The Project 25 Compliance Assessment Program (P25 CAP) provides equipment purchasers with demonstrated evidence of a product's compliance with a select group of requirements within the P25 suite of standards. The test procedures used to validate these requirements are also part of the P25 suite of standards. Although successful tests will demonstrate P25 compliance for the specific requirements tested, the conclusions drawn from these tests do not apply to every environment or individual user's needs. P25 CAP-mandated tests only demonstrate product compliance with the test procedures listed in the Supplier's Declaration of Compliance and, therefore, only attest to a product's compliance with specific requirements within the P25 standard.

Revision History

Version	Date	Description
Draft	12/21/16	Initial draft for public comment
1.0	03/01/17	Updated based on received public comments

Contents

This page is intentionally blank.

1 Non-Project 25 (P25) Standard Encryption Path Forward

The Project 25 Compliance Assessment Program Advisory Panel (P25 CAP AP) deliberated for many months concerning the wide-spread use of P25 subscriber unit equipment that includes non-P25 standard encryption without also including P25 standard AES 256 encryption. The P25 CAP AP forwarded its recommendation in the form of a resolution, found below, to the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office for Interoperability and Compatibility (OIC) for its consideration.

P25 equipment with only non-P25 standard encryption has caused interoperability challenges in the field. When multiple agencies need to communicate securely as a group, every subscriber unit in the group must use the same encryption algorithm and key. Matching keys can be loaded into the subscriber units in a straightforward manner, but the same encryption algorithm must be present in each subscriber unit before keys can be loaded.

The P25 standard encryption algorithm is AES 256. The TIA-102.AAAD-B Block Encryption Protocol document, originally published in July 2002, defines AES 256 for P25. On the federal side, AES 256 is a required encryption algorithm for a number of agencies, including DHS and the Department of Justice. The 2016 SAFECOM grant guidance recommends AES 256, and the Federal Communications Commission specifies the AES encryption algorithm for use in the 700 MHz Interoperability channels.

The P25 standard encryption algorithm before AES 256 was DES-OFB. The DES encryption algorithm standard has been 'broken' and is no longer considered strong enough for secure communications. The National Institute of Standards and Technology withdrew DES as a standard in May 2005.

Most equipment submitted to the P25 CAP includes the AES 256 encryption algorithm as an optional feature. The P25 CAP Suppliers' Declaration of Compliance (SDoC) and Summary Test Report (STR) documents indicate that encryption was an option when the approved equipment was tested, but public safety agencies can use grant funds to purchase P25 CAP approved equipment with or without the optional AES 256 encryption. P25 CAP AP has no intention of requiring the purchase of optional AES 256 encryption for all equipment acquired by grantees. A problem occurs, however, when the P25 equipment manufacturer provides a non-P25 standard encryption algorithm with the equipment when the optional AES 256 encryption is not ordered.

The P25 CAP AP wants to stop the practice of manufacturers providing subscriber units with a non-P25 standard encryption without also including P25 standard AES 256 encryption. OIC considers the following acceptable, if a vendor provides a radio with:

- No encryption;
- Standard encryption (AES 256); or
- Standard encryption and non-standard encryption.

This CAB addresses DHS OIC taking actions to stop this practice as part of the P25 CAP and to ask that manufacturers provide a path for public safety users to add AES 256 to fielded P25 subscriber units that

are now only equipped with non-P25 standard encryption. Specifically, this action should be taken for equipment bought with federal grants and those equipment purchases intended to be P25 CAP approved equipment.

2 P25 CAP AP Recommendation

The P25 CAP AP developed its recommendation for action and presented it during the P25 Steering Committee meeting at the October 2016 P25/Telecommunications Industry Association meetings in Philadelphia, Pennsylvania. The entire resolution appears below.

- **WHEREAS**, SAFECOM Grant Guidance specifies, "Ensure all P25-eligible equipment, features and capabilities selected are P25-compliant, to include new equipment and upgrades. When federal grant funds are used to purchase P25 land mobile radio equipment and systems that contain non-standard features or capabilities, while a comparable P25 feature or capability is available, grantees must ensure the standards-based feature or capability is included as well."
- **WHEREAS**, when a manufacturer provides a non-P25 standard encryption as a baseline feature, without providing a comparable P25 feature or capability, such as single key AES, this manufacturer's equipment is not in compliance with the SAFECOM Grant Guidance.
- **WHEREAS**, the wide-spread use and implementation of the non-P25 standard encryption in the manufacturers' radios has effectively destroyed the P25 multi-vendor sourcing environment the P25 CAP is required to protect.
- **WHEREAS**, multiple manufacturers have begun to provide and advertise non-P25 standard encryption variants to fairly compete with existing non-P25 compliant radios, further exacerbating the proliferation of non-P25 standard encryption in the P25 environment.
- **WHEREAS**, the P25 Compliance Assessment Program Advisory Panel (P25 CAP AP) recognizes that the wide use of non-P25 standard encryption requires that it must continue to be supported by the manufacturers until the P25 standard AES encryption can be implemented.
- **WHEREAS**, it is the Department of Homeland Security (DHS) Office of Interoperability and Compatibility (OIC)/P25 CAP AP's responsibility to protect an interoperable, multi-vendor, open P25 standard environment.
- **RESOLVED**, that the P25 CAP AP hereby RECOMMENDS that DHS OIC issue a clear ultimatum to any and all manufacturers providing the non-P25 standard encryption, that they must bring their radio equipment into compliance within 45 days of the issuance of such order or risk loss of Federal Fund Eligibility.
- Considering the above, the P25 CAP AP suggests that non-compliant manufacturers provide the P25 standard single-key AES for non-compliant radios.

3 OIC Path Forward

OIC accepts the P25 CAP AP recommendation. OIC believes focused actions should: (1) stop the continued manufacturer practice of providing non-P25 standard encryption without AES 256 encryption in equipment acquired by public safety; and (2) encourage manufacturers to provide P25 standard AES

256 encryption capability in fielded equipment. Going forward, a P25 product with non-P25 standard encryption and without P25 standard encryption AES 256 will not be approved by OIC.

OIC will take the following actions:

1) Review the existing 2010 SDoCs and STRs.

    - Check STR encryption test case results against equipment marketing materials to ensure that AES 256 is offered for the existing approved equipment if encryption test case results were 'P for pass.'
    - If equipment is found to have a 'P' result for an encryption test case result and the manufacturer does not offer AES 256 for that equipment, OIC will remove the associated STR and SDoC from the website and request the manufacturer submit a corrected 2010 SDOC/STR within 60 days stating "Unsupported" for the encryption.

2) Tighten the 2016 STR Compliance Assessment Bulletin (CAB) requirements.

    - Clearly specify that all encryption test cases must be conducted with P25 AES 256 encryption.
    - Require manufacturers to clearly state in the STR that AES 256 encryption was used for the conventional performance encryption test cases, as well as the conventional and trunking interoperability encryption test cases, and state if AES 256 encryption is an optional feature for the equipment under test.

3) Tighten the 2016 SDoC CAB requirements.

DHS OIC accepts two states for P25 CAP approved (grant-eligible) equipment with regards to encryption: (1) with the AES 256 encryption algorithm enabled and usable,[1] and (2) without any encryption at all (i.e., neither AES nor a non-standard algorithm).

A declaration section will be added to the SDoC where the manufacturer must declare which of the three model options are supported by the product or model class.

- Option 1 (Encryption)
  The product or model class has been tested with the P25 standard AES 256 encryption algorithm, the encryption test case results are 'P for pass' and shall be available with AES 256 installed when acquired. Other non-standard algorithms may also be included in addition to AES 256.
- Option 2 (No Encryption)
  The product or model class has been tested with the P25 standard AES 256 encryption algorithm and the encryption test case results are 'P for pass.' This product or model class shall be available without any voice privacy or non-AES 256 encryption algorithm installed when acquired.

[1] Manufacturers may choose to include another proprietary encryption algorithm in addition to the AES 256.

- Option 3 (No Encryption)
  The encryption test case results for this product or model class are 'U for unsupported.' This product or model class shall only be available without any voice privacy or non-AES 256 encryption algorithm installed when acquired (i.e., no encryption capability).

4) Make AES 256 encryption available for fielded equipment.

OIC shall encourage manufacturers to establish programs so public safety agencies with P25 standard equipment without P25 standard AES 256 encryption could add AES 256 to become P25 compliant, if the public safety agencies so desire.

OIC shall engage with manufacturers, one-on-one, to emphasize the need to provide a P25 standard encryption algorithm to enable interoperable, secure communications that are independent of location or public safety agency.

OIC shall notify the manufacturers of the proposed 'Tightened 2016 STR and SDoC' modifications and ensure their understanding before the 2016 SDoCs are submitted.

4 Implementation

To carry out these actions, OIC will publish their intentions to take corrective actions on the DHS S&T website, as well as via other communications methods. OIC has begun its assessment of the 2010 SDoCs and STRs. If OIC identifies an issue, it will alert the manufacturer and request that the manufacturer consider remedies and present its options to OIC within 60 days.

OIC stands ready to work with individual public safety agencies to ensure adherence to the spirit of the plans laid out in this document. If, after 60 days, the matter is not resolved to the satisfaction of OIC, OIC will remove the equipment in question from the P25 CAP approved (grant-eligible) equipment list.

This page is intentionally blank.