EFJohnson
TECHNOLOGIES
We Respond.

The Use of ADP Encryption in Federal Grant Funded Programs

Author: John Oblak
EF Johnson Technologies Vice President of Standards and Regulatory Affairs
Chair TIA TR-8 Committee on Mobile and Personal Private Radio Standards

June 20, 2011

Executive Summary:

Customers who desire encryption are frequently confused among their choices. EFJohnson's commitment to support interoperability is evident because we provide compliant and interoperable products, including encrypted products. Many customers are using some form of federal grant money from DHS or other entities; this grant money promotes interoperability and compatibility among emergency communications equipment. The use of encryption is becoming more prevalent.

This bulletin highlights the requirements for compatible and interoperable encryption offerings within Project 25 equipment and the advantages of our Project 25 products when compared to competitor offerings that may not fully satisfy the intent and spirit of interoperability as called out by the grant guidance and Project 25 requirements.

Technical Background:

Some manufacturers offer optional proprietary features in their Project 25 equipment. An example of this is a low cost encryption option, Advanced Digital Privacy (ADP). ADP is not part of the Project 25 suite of standards. Rather, it is a proprietary encryption scheme developed to meet the needs of low end encryption users. However, when a customer purchases and deploys equipment with ADP they are locked in to buying additional subscriber equipment only from that single supplier.

ADP is not part of the Project 25 suite of standards.

The standard for Project 25 encryption is Advanced Encryption Standard (AES).

Encryption schemes are classified as to their usage. Generally, the higher number corresponds to weaker encryption. ADP is considered a Type IV encryption for use in commercial or other communications, and uses a 40 bit key sequence. The standard for Project 25 encryption is Advanced Encryption Standard (AES), which is a Type III algorithm, defined for use in unclassified but sensitive government communications. AES uses a 256 bit key sequence. With its smaller key sequence, ADP is a weaker encryption algorithm than AES, and as such, does not meet the security requirements of the federal government for their encryption needs. All federal encryption needs mandate the use of AES encryption.

The Project 25 Statement of Requirements document allows for proprietary implementation of features, but states "manufacturers shall implement P25-compliant features whenever equivalent proprietary features are implemented[1]." The intent of this statement is to ensure that equipment has the capability of providing interoperable operation, even if proprietary features are implemented. The wording of the Statement of Requirements requires implementation of the Project 25 compliant feature, but does not state that the feature is required to be supplied with every product. In some cases, manufacturers are marketing proprietary features in their product, without providing the corresponding Project 25 compliant feature.

What Does This Mean to Us and to Our Customers?

When radios are purchased with federal grant money through DHS or other agency, grant guidance is provided. With respect to encryption, the SAFECOM grant guidance states "To ensure encrypted interoperability, the P25 suite of standards references the use of Advanced Encryption Standard (AES) in the Project 25 Block Encryption Protocol, ANSI/TIA-102.AAD. Entities pursuing encrypted communications capabilities must be compliant with the P25 Block Encryption Protocol[2]." The SAFECOM grant guidance makes it clear that encrypted radios purchased through federal grant funding must be supplied with the Project 25 compliant AES encryption algorithm.

The SAFECOM grant guidance makes it clear that encrypted radios purchased through federal grant funding must be supplied with the Project 25 compliant AES encryption algorithm.

EFJohnson offers an additional encryption, DES-OFB, on many of its products at no cost. DES-OFB is an encryption algorithm that previously was the Project 25 standard encryption algorithm. However, the federal government discontinued the use of DES-OFB in favor of the more secure AES. EFJohnson provides the DES-OFB encryption in its products to allow for interoperability with many of the previously deployed encrypted radios. However, unlike ADP, the DES-OFB algorithm is standardized, and is recognized in the Project 25 standards as a legacy feature. Radios purchased with DES-OFB encryption do not violate grant guidance because it is not proprietary.

Summary

In summary, radios with ADP encryption alone <u>do not qualify</u> under the SAFECOM grant guidance for federal grant funding. Such products do not meet the requirements for federal usage, and lock the customer into purchasing an inferior encryption from a single supplier. EFJohnson remains committed to providing Project 25 compliant products that meet the requirements for compatibility and interoperability.

[1] APCO Project 25 Statement of Requirement, March 3, 2010

[2] FY 2011 SAFECOM Guidance on Emergency Communications Grants: http://www.safecomprogram.gov/NR/rdonlyres/7C73CFA8-DC8B-487C-82A0-42BD7C06F3BA/0/FY_2011_SAFECOM_Guidance_121510.pdf