Commercial Encryption to secure your Telemetry Data

Paul Cook
Product Line Manager, RF Products
Curtiss-Wright, Aerospace Instrumentation
Newtown, PA
pcook@curtisswright.com

ABSTRACT

In the United States, the telemetry industry has traditionally relied on the National Security Agency (NSA) to provide leadership and/or solutions to encrypt telemetry data for streaming applications. However, with the current heightened concern to protect data for programs with short development cycles, encryption solutions based on the commercial Advanced Encryption Standard (AES) algorithms offer options that augment the NSA solutions. This paper describes the development of an encryption – decryption module, and the attendant trades in using (AES) block-cipher based encryption algorithm for streaming applications, resulting link performance, and the certification choices and requirements.

INTRODUCTION

As the world realizes that all of our data is at risk of being exploited by individuals outside of our country, we are under pressure to protect all of our data, no matter the classification. Recent communications at Curtiss Wright has mandated the encrypting of all data. Previously, the National Security Agency handled the Telemetry requirement with their preferred solution as a doctrine to encrypt all transmitted telemetry data. This system has worked well over the years but is not practical for data in transit that is not classified, or for data that is considered private. What else is available today that provides data privacy without requiring the NSA oversight and control?

Why do we encrypt?

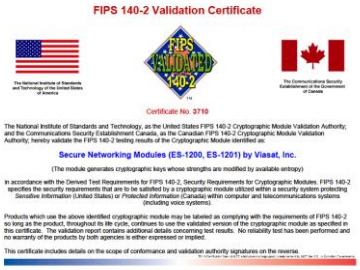
We encrypt data to protect it from open access to the information. Data in transit, whether through an ethernet port, or through a transmitter the information must be protected from those who choose to exploit it. There are many forms of encryption, at different levels of strength, and are used daily from logging into your computer, to banking via an ATM machine, as well as high assurance equipment that provide the maximum protection from inappropriate access.

Certifications and what are they?

There are two forms of certifications the commercial side through the National Institute of Standards and Technology (NIST) as well as through the National Security Agency. For telemetry, there were always two programs that supported the telemetry specific certification to include a Commercial COMSEC Endorsement Program (CCEP) and a User partnership program

(UPA) that fulfilled all of our program requirements for Telemetry. The latest change in this process includes a commercial solutions for classified (CSFC) and a popular alternate approval path. The CSFC focuses on a suite B encryption solution or AES-256 with various combination of software and hardware implementations appropriate with the use case.

NIST also provides a process of certifying encryption devices similar to the processes within the NSA. NIST uses a third-party lab to evaluate the encryption process, the key management process, along with other dedicated test to complete the Federal Information Processing Standard [1] (FIPS-140-2) certification at one of four levels of security.


FIPS 140-2 Validation Certificate

Certificate No. 3710

Secure Networking Modules (ES-1200, ES-1201) by Viasat, Inc.

Figure 1 NIST Certification for the MESP-100-1

Does the MESP Interface support the telemetry application?

Telemetry has been encrypting their data since the late 1970s as a result of a mandate that all telemetry data will be made secure during transmission. Much of the unclassified data has historically been transmitted in the clear. The Curtiss Wright MESP-100-1 was developed for the telemetry use case where a PCM encoder generating the Chapter 4 data, encrypting the data and then transmitting the data in a secure fashion. The MESP incorporates a NIST certified device from a well-known vendor of secure crypto modules and implemented in a traditional form factor including interfaces. This allows for the telemetry community to secure their unclassified data with the interfaces they are accustom to from the NSA implementation.

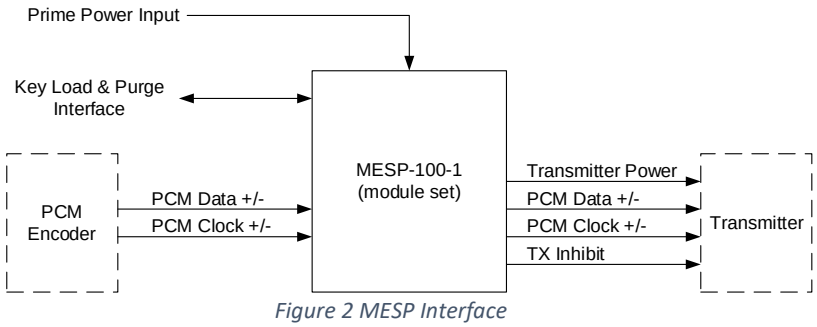


Figure 2 MESP Interface

What Mechanical options to increase the use case of the MESP are there?

The mechanical design of the MESP serves two purposes. The first is a stand-alone module that can be wired to a data source including both clock and data, prime power, and a typical transmitter interface. The term stand-alone points to an option to place this small stack into any open space supporting a late decision to encrypt the unsecure data as we are experiencing now. An alternate solution is to embed the encryption capability where the MESP can be stacked on a standard miniature PCM encoder as shown in Figure 3.

Figure 3 Mechanical Configurations

Once you encrypt, you must decrypt!

Normally the ground decryption takes the form of a rack mount box with the specific ground telemetry interfaces as in a single ended TTL with 50-ohm drive capability. The MESP provides both the encrypt and decrypt interface in one assembly. In practice the decryption operation is provided in a 19-inch rack assembly and also provides an encryption interface to support any post securing of the data if or when it is desired. The advantage of have both encryption and decryption in one assembly is the ability to loop back the data providing high assurance of the operation of the equipment.

Figure 4 Rack mounted decryption device

The encrypt-decrypt function of the MESP also supports a bi-directional secure transmission when using two MESP devices and standard transmitter – receiver pairs provide the RF connection in both directions sending the data in a secure manner.

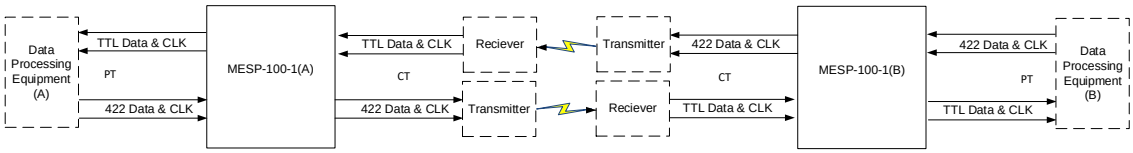


Figure 5 Bi-direction secure link

What options are there for obtaining the keying material?

Keying material starts with a key specification that defines the key structure. NSA or a private company depending of the type of algorithm, will generate the keying material. Recalling a story being told from an NSA official, on a company who attempted to use AES for the first time in a telemetry application but was not fully aware of a key structure or what it takes to generate a formal NSA key. Never forgetting that story, the Curtiss Wright team created a source for the MESP key as well as software to generate the material to avoid the availability issues. The software suite also provides a key management functionality is addition to generation and destruction.

Figure 6 Key management software

What is the MESP performance compared to other solutions?

The MESP series of modules are designed to support up to 20 Mbps with data latencies in less than 600-microseconds. Performance in terms of a link margin is similar when randomization is used in loosing a couple of dB in the link. The MESP embedded device has some forward error correction capability which gains back the couple dB of loss in the link. In some cases, whether the link starts to fade, the additional two dB can make the difference between error free performance and large loss of PCM sub frames. Personally, when performing a link analysis, it should always provide at least 10 dB of additional margin to account for unanticipated RF cable loss, data loss due to link fades or interference in the system.

CONCLUSION

The MESP was developed to provide data privacy for exportable equipment for various platforms that fall outside of the US. Lately a second use case has been discovered in securing all data being transmitted on test ranges. This allows the user to avoid the additional controls associate with a NSA short title but yet provides an certified solution for secure transmission of the data. As always guarding the data is paramount and when considering using the MESP a program approval would be warranted.

REFERENCES

[1] FIPS-140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES 2002 December 03 U.S. Department of Commerce National Institute of Standards and Technology, Gaithersburg, MD 20899