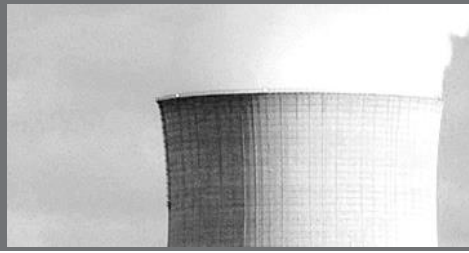
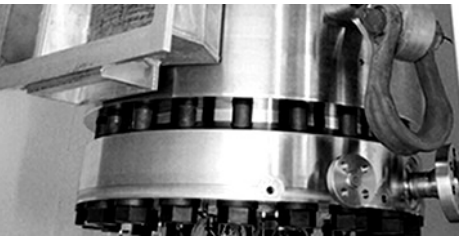
Exportable Encryption

Paul Cook





Biography

Director of missile systems and Product line manager at Teletronics Technology Corporation, a Curtiss Wright company. He is responsible for all RF products and flight safety systems including transmitters, receivers, transponders, termination receivers, and recently telemeter systems. Paul has various engineering and business degrees and has held similar positions at L-3 Technologies, Aydin Vector Corporation and at General Dynamics Corporation. Paul has over 40 years of Telemetry experience.

Overview – Exportable Encryption

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 around the world has increased. With short development cycles, encryption solutions based on the commercial Advanced Encryption Standard (AES) algorithms offer options that augment the US only, NSA solutions.

This presentation provides a high-level overview of exportable 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.

Export Control

What does Exportable mean?

- Two agencies in the US for Export Control
  - International Traffic and Arms Regulation (ITAR) for items listed in the US Munitions List (USML)
  - Export Administration Regulation licensing operated by the Commerce Department
- Military, Commercial, and Dual use items
- Hardware, Software, Technology, Service

2013 a rewrite of the USML moved 95% of the Telemetry application equipment from ITAR to Commerce

- Very few items for Telemetry are ITAR today
  - COTS Telemetry hardware are generally considered dual use (must provide clear intend during the early decision to productize an item)
  - Specifically design for an end item on the Munitions list
- The MESP is approved under Commerce licensing as ECCN 5A002 a.1
  - Information security" systems, equipment and "components" .a – Designed or modified to use 'cryptography for data confidentiality' having 'in excess of 56 bits of symmetric cryptographic strength key length, or equivalent', where that cryptographic capability is usable without "cryptographic activation" or has been activated, as follows:
  - a.1 Items having "information security" as a primary function
  - a.2 Digital communication or networking systems, equipment or components, not specified in paragraph 5A002.a.1.;
  - a.3 Computers, other items having information storage or processing as a primary function, and components therefor, not specified in paragraphs 5A002.a.1. or 5A002.a.2.; N.B. For operating systems, see also 5D002.a.1. and 5D002.c.1.
  - a.4 - Items, not specified in paragraphs 5A002.a.1. to a.3., where the 'cryptography for data confidentiality' having 'in excess of 56 bits of symmetric cryptographic strength key length, or equivalent' meets all the following: a. It supports a non-primary function of the item; and
- Country Code Restrictions National Security 1 Anti Terrorism 1 (includes Ireland)
  - 3 See § 742.6(a)(3) for special provisions that apply to "military commodities" that are subject to ECCN 0A919.
  - 4 See § 742.6(a)(2) and (4)(ii) regarding special provisions for exports and re-exports of certain thermal imaging cameras to these countries.

Why do we encrypt?

- As the world realizes that all our data is at risk of being exploited by individuals outside of our country, we are under pressure to protect that 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
- 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.

Certification

Exportable Encryption

- Crypto Modernization
  - Suite A – US only
  - Suite B – AES-256 based for NATO and friendly countries
- Based on AES-256
  - ViaSat's ES-1200 Module, renamed as the ES-1201 and NIST Cerified

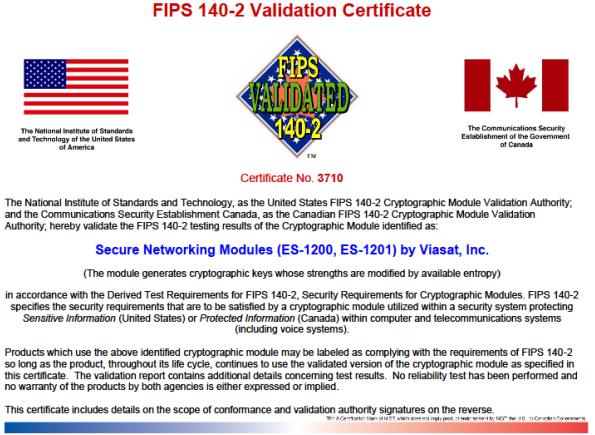
There are two forms of certifications the commercial side through the National Institute of Standards and Technology (NIST) as well as through the National Security Agency.

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 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's Crypto Variable (CV) validation testing.

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

The National Institute of Standards and Technology of the United States of America

FIPS VALIDATED 140-2

The Communications Security Establishment of the Government of Canada

Certificate No. 3710

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

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

(The module generates cryptographic keys whose strengths are modified by available entropy)

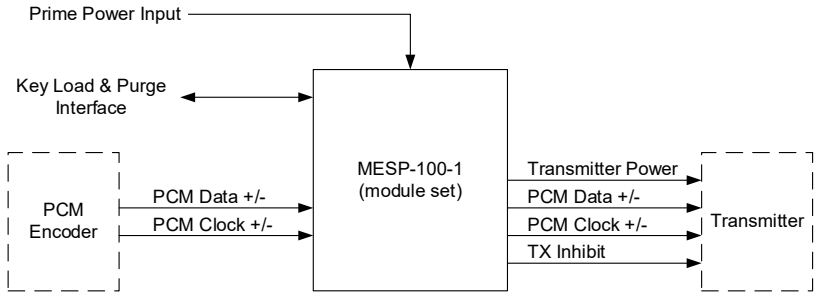
in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

Encryption for Telemetry

- **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 ViaSat and implemented in a traditional telemetry form factor including interfaces**
- **This allows for the telemetry community to secure their data with the interfaces they are accustomed to from the NSA implementation**

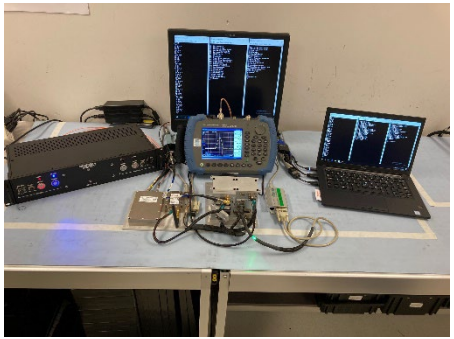


Intended “use-cases”

- **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**

MCDAU Stacks

Miniature Airborne Telemetry System



Dual Encryption Stack

Where 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 provides an encryption interface to support any post securing of the data if or when it is desired

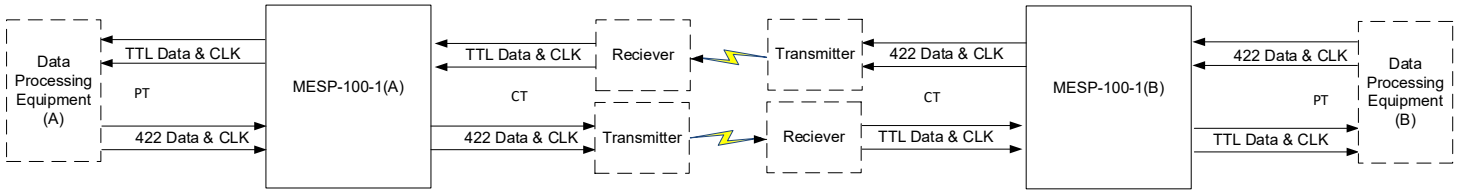
The advantage of have both encryption and decryption in one assembly is the ability to loop back the data providing high assurance of the operation of the equipment

Dual Encryption Stack

Dual Decryption Rack mounted unit

Alternate usage for the MESP

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



Keying Material

- **Keying material starts with a key specification that defines the key structure**
- **NSA or a private company depending on 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**

High Level Performance Characteristics

The MESP series of modules are designed to support up to 20 Mbps with data latencies in less than 0.6 microseconds

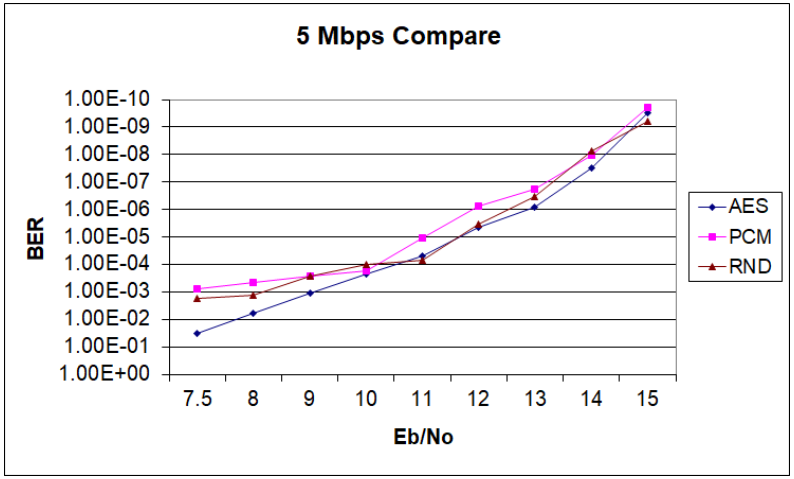
Supports simultaneous encryption and decryption capability

Performance in terms of a link margin is similar when randomization is used in loosing a couple of dB in the link

Output rated current rating of the transmitter interface is 3 amperes

The MESP embedded device has some forward error correction capability which gains back the couple dB of loss in the link (1.083 data rate multiplier)

Operates over the standard environmental specification from the miniature DAU product line



BER comparison (PCM/FM)

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 an NSA short title but provides a 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**

Paul Cook
PCook@curtisswright.com
P: 267.352.2018
M: 609.694.0344